PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-295801

(43)Date of publication of application : 10.11.1995

(51)Int.Cl. G06F 9/06
G06F 12/14
G09C 1/00

(21)Application number : 07-090443

(22)Date of filing : 17.04.1995

(71)Applicant : INTERNATL BUSINESS MACH CORP <IBM>

(72)Inventor : COOPER THOMAS E
PHILIPS HUDSON W
PRYOR ROBERT F

(30)Priority

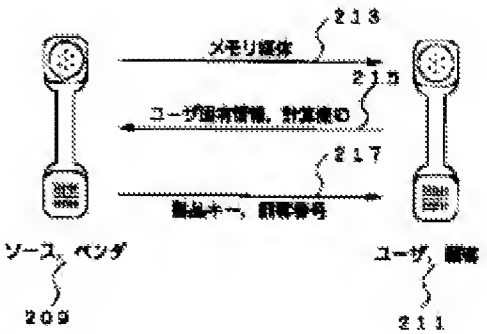
Priority number : 94 235032 Priority date : 25.04.1994 Priority country : US

(54) DISTRIBUTION METHOD OF SOFTWARE OBJECT

(57)Abstract:

PURPOSE: To provide a method and device to distribute a software object from a source to a user.

CONSTITUTION: The software object is ciphered by a ciphering operation using a successive ciphering key. The software object is sent from a source 209 to the user 211 and loaded to a data processing system for user control with a specific configuration. At least a computer ID 215 consisting of a specific data processing system of the data processing system of user control is led out from at least a part of the object. Furthermore, at least a temporary key 217 based on a successive ciphering key and the computer ID 215 are led out from a part of the object. Since the successive key generating program is served to receive the temporary key 217 to generate a successive ciphering key, the user 211 uses the temporary key 217 for a prescribed period to access the software object thereby generating the successive ciphering key.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平7－295801

(43)公開日　平成７年(1995)11月10日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ	9/06	５５０　Ｃ	7230－5B		
	12/14	３２０　Ｂ			
		Ｆ			
Ｇ０９Ｃ	1/00		9364－5L		

審査請求　未請求　請求項の数８　ＯＬ　（全 31 頁）

(21)出願番号　特願平7－90443

(22)出願日　平成７年(1995)４月17日

(31)優先権主張番号　２３５０３２

(32)優先日　1994年４月25日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレイション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）

(72)発明者　トーマス・イー・クーパー
アメリカ合衆国80027　コロラド州ルイヴィル　ウエスト・ウィロウ・ストリート　858

(74)代理人　弁理士　合田　潔　（外２名）

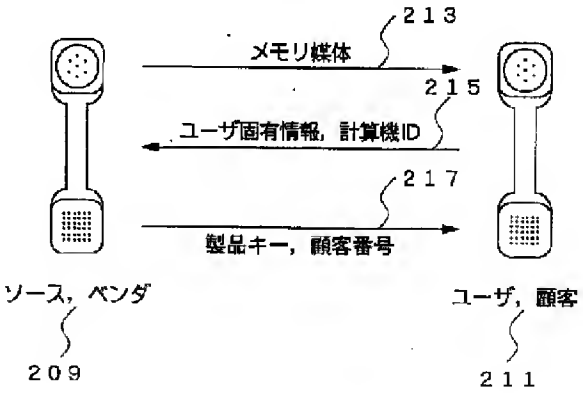
最終頁に続く

(54)【発明の名称】　ソフトウェア・オブジェクトの配布方法

(57)【要約】

【目的】　ソースからユーザにソフトウェア・オブジェクトを配布するための方法および装置を提供する。

【構成】　ソフトウェア・オブジェクトは永続暗号化キーを使用する暗号化操作で暗号化される。このソフトウェア・オブジェクトは、ソースからユーザに送られ、特定の構成を有するユーザ制御のデータ処理システムにロードされる。少なくとも一部がユーザ制御のデータ処理システムの特定のデータ処理システム構成に基づく計算機ＩＤが導出される。また、少なくとも一部が計算機ＩＤと永続暗号化キーに基づく一時キーが導出される。一時キーを受け取って、永続暗号化キーを生成するために永続キー生成プログラムが提供されるので、ユーザは、ソフトウェア・オブジェクトにアクセスするために、所定の期間、一時キーを使用して永続暗号化キーを生成することができる。



【特許請求の範囲】
【請求項１】供給側であるソースからユーザにソフトウェア・オブジェクトを配布する方法において、
永続暗号化キーを使用する暗号化操作で前記ソフトウェア・オブジェクトを暗号化するステップと、
前記ソースから前記ユーザに前記暗号化ソフトウェア・オブジェクトを送るステップと、
特定のシステム構成を有するユーザ制御のデータ処理システムに前記暗号化ソフトウェア・オブジェクトをロードするステップと、
少なくとも一部が前記システム構成に基づく計算機ＩＤを導出するステップと、
少なくとも一部が前記計算機ＩＤと前記永続暗号化キーとに基づく一時キーを導出するステップと、
所定の期間、前記ユーザが前記一時キーを使用して前記永続暗号化キーを生成できるように、前記一時キーを受け取って、前記永続暗号化キーを生成するための永続キー生成機能を動作させ、前記ソフトウェア・オブジェクトへのアクセスを可能にするステップとを含む方法。
【請求項２】前記暗号化ソフトウェア・オブジェクトが、コンピュータがアクセス可能なメモリ媒体上に記録されて、前記ソースから前記ユーザに送られる、請求項１に記載のソフトウェア・オブジェクトを配布する方法。
【請求項３】前記永続キー生成機能が、前記コンピュータがアクセス可能なメモリ媒体上に保持され、前記暗号化ソフトウェア・オブジェクトとともに前記ソースから前記ユーザに送られる、請求項２に記載のソフトウェア・オブジェクトを配布する方法。
【請求項４】前記永続キー生成機能をその構成要素として含む、ファイル管理プログラムを、　前記暗号化ソフトウェア・オブジェクトとともに前記ソースから前記ユーザに送るステップをさらに含む、請求項１に記載のソフトウェア・オブジェクトを配布する方法。
【請求項５】少なくとも前記一時キーを記録するために前記ユーザ制御のデータ処理システム内にキー・ファイルを作成するステップを含む、請求項１に記載のソフトウェア・オブジェクトを配布する方法。
【請求項６】少なくとも１つの固有のシステム属性を暗号化キーとして使用して、前記キー・ファイルを暗号化するステップを含む、請求項５に記載のソフトウェア・オブジェクトを配布する方法。
【請求項７】作成者からユーザにソフトウェア・オブジェクトを配布する方法において、
永続キーを使用して前記ソフトウェア・オブジェクトを暗号化するステップと、
前記ソフトウェア・オブジェクトをコンピュータがアクセス可能なメモリ媒体にファイル管理プログラムとともに記録するステップと、
前記作成者から前記ユーザに前記コンピュータがアクセス可能なメモリを発送するステップと、
前記ファイル管理プログラムをユーザ制御のデータ処理システムにロードし、それを前記ユーザ制御のデータ処理システム用のオペレーティング・システムに関連付けるステップと、
前記ファイル管理プログラムを使用して、前記ユーザ制御のデータ処理システムの少なくとも１つの属性に基づく計算機ＩＤを導出するステップと、
前記ユーザ制御のデータ処理システムで前記コンピュータがアクセス可能なメモリを読み取るステップと、
少なくとも一部が前記計算機ＩＤに基づく一時キーを導出するステップと、
前記ユーザ制御のデータ処理システムで前記ファイル管理プログラムを実行することにより、前記一時キーによって定義される期間の間、前記ソフトウェア・オブジェクトへのアクセスを制限するステップと、
前記ユーザ制御のデータ処理システムにおいて永続キー生成機能を実行することにより、少なくとも前記一時キーを受け取ったことに対する応答として前記永続キーを提供するステップとを含む方法。
【請求項８】前記ファイル管理プログラムが、前記ユーザ制御のデータ処理システムによって実行されるときに、複数の動作モードで動作可能であり、（ａ）前記一時キーを使用することで前記ソフトウェア・オブジェクトが一時的に使用可能になる一時試用動作モードと、（ｂ）前記ソフトウェア・オブジェクトを永続的に使用可能にして、前記ユーザによる前記ソフトウェア・オブジェクトの無制限使用を可能にする永続使用動作モードとを含むことを特徴とする、請求項７に記載のソフトウェア・オブジェクトを配布する方法。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は、一般的にはソフトウェア・オブジェクトへのアクセスを保護するための技法に関し、より具体的にはソフトウェア・オブジェクトへのアクセスを一時的に暗号化し制限するための技法に関する。
【０００２】本発明は、"Method and Apparatus for Enabling Trial Period Use of Software Products: Method and Apparatus for Utilizing a Decryption Stub"という名称の米国特許出願第２３５０３３号、"Method and Apparatus for EnablingTrial Period Use of Software Products: Method and Apparatus for Allowing a Try-and-Buy User Interaction"という名称の米国特許出願第２３５０３５号、"Method and Apparatus for Enabling Trial Period Use of Software Products: Method and Apparatus for Utilizing an Encryption Header"という名称の米国特許出願第２３５０３１号、および"Method and Apparatus for EnablingTrial Period Use of Software Products: Method and Apparatus for

Allowing the Distribution of Software Objects″という名称の米国特許出願第２３８４１８号に関連するものである。

【０００３】

【従来の技術】ソフトウェア製品の作成と販売により、革新的な製品を有する企業に対して莫大な富が生み出されてきたが、時間が経つにつれて消費者がコンピュータに詳しくなるので、この傾向は今後も継続するものと考えられる。潜在的ユーザには市販されている様々な製品を走査検索する機会がほとんど与えられないため、コンピュータ・ソフトウェアは販売しにくいものである。通常、ソフトウェア製品はプラスチック・フィルムで収縮包装された箱に収められており、潜在的顧客には、購入前に実際にそのソフトウェアを操作または体験する機会がほとんどまたはまったく与えられない。このため、消費者は、満足できるソフトウェア製品が見つかるまで複数の製品を次々に購入せざるを得ない場合が多く、製品に対する不満が募ってくる。これは、この世界で大量の海賊版ソフトウェアが発生している重大な原因の１つたりうる。潜在的ソフトウェア購入者は、ソフトウェアの一時使用という明白な意図を持って、友人や同僚から１組のディスケットを「借りる」ことが多い。しかし、このような一時使用が長期間にわたり、潜在的顧客が実際にはソフトウェア製品を購入せず、借りたコピーに頼る可能性も多いだろう。

【０００４】映画館には映画の予告編があり、テレビにはコマーシャルがあるが、ソフトウェア製品のサンプリングにはこのような共通の伝達経路が存在しないため、ソフトウェア・メーカは、新製品を宣伝し、新たな顧客を勧誘するために、印刷物やダイレクトメールによる宣伝に頼らざるを得ない。しかし、残念ながら、静的な印刷形式ではユーザと製品との対話をシミュレートすることができないため、印刷物は正確に製品を説明できない場合が多い。コンピュータ・ソフトウェア製品を購入するかどうか決心する前に顧客がその製品にアクセスでき、製品を違法使用する危険性を伴わずにこれを実現できるのであれば、ソフトウェア製品のメーカも顧客もどちらも十分要求が満たされるはずである。

【０００５】暗号化したソフトウェア製品の配布は、購入前に潜在的ユーザに製品を配布するためにソフトウェア・ベンダが利用できる機構の１つであるが、製品へのユーザ・アクセスを可能にするキーを配布しなければならない。この場合、ベンダは、潜在的顧客の正直さと誠実さに完全に頼らざるを得ない。つまり、無節操な人や誠意のない人であれば、その友人や同僚にキーを渡し、無許可アクセスを可能にする恐れがある。さらに、無節操な人は、多数の人が無許可ユーザになれるように、一般の人がアクセス可能な掲示板にキーを掲載してしまう可能性もある。通常、このような安全保護違反は容易に防止することができないため、ベンダは潜在的顧客による試用のためにソフトウェアを配布することを躊躇してきた。

【０００６】

【発明が解決しようとする課題】本発明の一目的は、一時的な試用期間を超えて海賊行為や無許可利用が行われるという不必要な危険性にソフトウェア製品を曝さずにユーザに一時的な試用期間を許可することを特徴とする、作成者から潜在的ユーザにソフトウェア・オブジェクトを配布するための方法および装置を提供することにある。

【０００７】本発明の他の目的は、永続暗号化キー（long-lived encryption key）を使用してソフトウェア・オブジェクトが暗号化され、ソースからユーザに送られることを特徴とする、ソースからユーザにソフトウェア・オブジェクトを配布するための方法および装置を提供することにある。

【０００８】本発明の他の目的は、コンピュータがアクセス可能なメモリ媒体に格納された特定のファイルへのアクセスを保護するための、データ処理システム内の方法および装置を提供することにある。

【０００９】本発明の他の目的は、コンピュータがアクセス可能なメモリ媒体に格納された特定のファイルへのアクセスを保護するための、データ処理システム内の方法および装置を提供することにある。

【００１０】本発明の他の目的は、ソースからユーザにソフトウェア・オブジェクトを配布するための方法および装置を提供することにある。この場合、コンピュータがアクセス可能なメモリ媒体がソースから潜在的ユーザに配布される。

【００１１】

【課題を解決するための手段】本発明の第一の目的は、好ましくは、ソフトウェア・オブジェクトをファイル管理プログラムとともにコンピュータがアクセス可能なメモリ媒体で提供することで達成される。このソフトウェア・オブジェクトは、１つまたは複数の特定の暗号化操作により取消し可能な機能制限が施されていることが好ましい。コンピュータがアクセス可能なメモリ媒体は、従来の郵便および配送サービスを使用して作成者から潜在的ユーザに発送される。潜在的ユーザは、これを受け取ると、ユーザ制御のデータ処理システムにファイル管理プログラムをロードし、そのデータ処理システム用のオペレーティング・システムにそれを関連付ける。次に、ユーザ制御のデータ処理システムを使用してコンピュータがアクセス可能なメモリ媒体が読み取られる。ファイル管理プログラムは、ユーザ制御のデータ処理システムによって実行され、定義済みの一時試用期間の間、ソフトウェア・オブジェクトへのアクセスを制限するよう機能する。一時試用動作モードの間、ソフトウェア・オブジェクトの取消し可能機能制限を取り消すことで、ソフトウェア・オブジェクトが一時的に使用可能にな

る。これは、ユーザ制御のデータ処理システムのオペレーティング・システムがソフトウェア・オブジェクトを呼び出したときの暗号化ソフトウェア・オブジェクトの暗号解読によって達成されることが好ましい。ファイル管理プログラムは、オペレーティング・システムによって呼び出されたときに暗号化ソフトウェア・オブジェクトを一時的に解読するように、コピー操作を防止することが好ましい。潜在的ユーザがソフトウェア・オブジェクトの購入を選択した場合は、永続使用動作モードに入り、そこでソフトウェア・オブジェクトの機能制限が永続的に取り消され、潜在的ユーザがソフトウェア・オブジェクトを無制限に使用できるようになる。これにより、潜在的ユーザがソフトウェアを検討して、そのソフトウェアが自分のニーズに合っているかどうかを判定できるようにするためのブラウズ操作が容易になる。

【００１２】ファイル管理プログラムは、ユーザ制御のデータ処理システムのオペレーティング・システムを連続監視し、システムの入力呼出しと出力呼出しを操作する。また、ファイル管理プログラムは、ユーザ制御のデータ処理システムのオペレーティング・システムが試用期間中にブラウズの対象となるソフトウェア・オブジェクトを要求した時点を識別する。その後、ファイル管理システムは、そのソフトウェア・オブジェクトに関連する一時アクセス・キーを取り出し、その一時アクセス・キーを検査して有効かどうかを判定する。次に、ファイル管理プログラムは、ソフトウェア・オブジェクトの機能制限を取り消し、処理のためにそれをデータ処理システムに渡す。

【００１３】暗号化したソフトウェア・オブジェクトは、特定のシステム構成を有するユーザ制御のデータ処理システムにロードされる。その後、少なくとも一部がユーザ制御のデータ処理システムの特定の構成に基づく数値計算機ＩＤ（numerical machine identification）が導出される。次に、少なくとも一部がこの数値計算機ＩＤと永続暗号化キーに基づく一時キーが導出される。この一時キーを受け取って永続暗号化キーを生成するための永続キー生成プログラムが提供されている。この一時キーを使用すると、ユーザはソフトウェア・オブジェクトにアクセスするための永続暗号化キーを所定の期間、生成することができる。これらの操作は、複数のモードで動作可能なファイル管理プログラムによって主に実行される。このようなモードとしては、セットアップ動作モード、計算機ＩＤ動作モード、一時キー導出動作モードがある。セットアップ動作モード時には、ファイル管理プログラムがユーザ制御のデータ処理システムにロードされ、ユーザ制御のデータ処理システム用のオペレーティング・システムに関連付けられる。計算機ＩＤ動作モード時には、少なくともユーザ制御のデータ処理システムの属性に基づく数値計算機ＩＤを導出するためにファイル管理プログラムが使用される。一時キー導出動作モード時には、少なくとも一部が数値計算機ＩＤに基づく一時キーが導出される。また、ファイル管理プログラムにより試用動作モードも可能になり、そのモードでは、一時キーによって定義された期間の間、ソフトウェア・オブジェクトへのアクセスを制限するためにユーザ制御のデータ処理システムでファイル管理プログラムを実行することでそのファイル管理プログラムが使用され、その定義済み期間中は、一時キーを含む少なくとも１つの入力の受取りに対する応答として永続キーを提供するために、ユーザ制御のデータ処理システムで永続キー生成プログラムが使用される。

【００１４】ファイル管理プログラムは、データ処理システムのオペレーティング・システム構成要素として提供される。コンピュータがアクセス可能なメモリ媒体には、少なくとも１つの暗号化ファイルと少なくとも１つの非暗号化ファイルとを含む複数のファイルが格納されている。それぞれの暗号化ファイルごとに、事前選択部分がコンピュータ・メモリに記録され、ファイルの暗号解読に使用できる情報を含む暗号解読ブロックが生成され、コンピュータ・メモリの他の場所にすでに記録されていた事前選択部分の代わりにその暗号解読ブロックがファイルに組み込まれる。ここでファイル管理プログラムを使用して、アクセス可能なメモリ媒体に格納されている被呼ファイルに関するコンピュータのデータ処理操作呼出しを監視する。ファイル管理プログラムは、その被呼ファイルが関連の暗号解読ブロックを備えているかどうかを判定する。被呼ファイルが関連の暗号解読ブロックを備えているかどうかに応じて、ファイル管理プログラムはその被呼ファイルを特定の方法で処理する。暗号解読ブロックを組み込んでも暗号化ファイルのサイズは変わらないため、所与のタイプの処理エラーが防止される。試用期間中、暗号化ファイルは暗号化状態に維持されるため、コピーすることができない。潜在的ユーザがソフトウェア製品の購入を決定した場合、暗号解読ブロックの代わりに事前選択部分をファイルに戻すための永続キーが提供される。暗号解読ブロックが除去されると、暗号化ファイルを暗号解読して、購入者による無制限使用を可能にすることができる。オペレーティング・システムによって呼び出されたときにファイルを代行受信するために、ならびに、暗号解読ブロックを使用してキー・ファイル用の名前を導出し被呼ファイルを読み取るために、ファイル管理プログラムを使用することが好ましい。それぞれの暗号化ファイルの暗号解読ブロックは、ファイル管理プログラムによって暗号解読され、被呼ファイル用の選択済みセグメントと比較されて、そのキーが特定のファイルを暗号解読できるかどうかを判定するための妥当性検査セグメントを含んでいる。暗号解読された妥当性検査セグメントが既知のクリア・テキスト妥当性検査セグメントと一致すると、ファイルは、今後の処理のためにオペレーティング・システムに渡され

るときに動的に暗号解読される。

【００１５】ファイル管理プログラムは、データ処理システムのオペレーティング・システム構成要素として提供される。データ処理システムにとって使用可能でコンピュータがアクセス可能なメモリ媒体には、少なくとも１つの暗号化ファイルと１つの非暗号化ファイルが格納されている。この暗号化ファイルには、少なくとも一部が実行可能コードで構成されている非暗号化安全保護スタブが関連付けられている。ここでファイル管理プログラムを使用して、コンピュータがアクセス可能なメモリ媒体に格納されている被呼ファイルに関するデータ処理システム呼出しを監視し、その被呼ファイルが関連の非暗号化安全保護スタブを備えているかどうかを判定し、被呼ファイルが関連の非暗号化安全保護スタブを備えているかどうかに応じて、その被呼ファイルを特定の方法で処理する。より具体的には、被呼ファイルが関連の非暗号化安全保護スタブを備えてないと判定された場合、その被呼ファイルの処理が可能になる。しかし、被呼ファイルが関連の非暗号化安全保護スタブを備えていると判定された場合には、被呼ファイルの処理が可能かどうかの判定を行う前にそのファイルを検査しなければならない。まず、暗号解読操作を実行可能にする情報を得るために、非暗号化安全保護スタブが検査される。次に、暗号解読操作が実行される。最後に、今後の処理のために被呼ファイルの転送が可能になる。被呼ファイルは、処理のためにオペレーティング・システムに渡されるときに動的に暗号解読されることが好ましい。また、被呼ファイルの実行前に非暗号化安全保護スタブが被呼ファイルから分離される。ただし、非暗号化安全保護スタブがたまたま被呼ファイルに接続されたままになってしまった場合には、処理操作を停止しなければならず、プロセッサがロック状態になるのを防止するため、メッセージを通知しなければならない。

【００１６】コンピュータがアクセス可能なメモリ媒体は、所定の暗号化エンジンと永続秘密キーとを使用して暗号化されるソフトウェア・オブジェクトを含んでいる。ソースとユーザとの対話を容易にするためのインタフェース・プログラムが提供される。このインタフェース・プログラムは、少なくともユーザ制御のデータ処理システムの所定の属性を使用して計算機ＩＤを生成する計算機ＩＤモジュールを含んでいる。また、このインタフェース・プログラムは、少なくとも一時キーを入力として受け取り、永続秘密キーを出力として生成する永続秘密キー生成プログラムをさらに含んでいる。一時キーをテストしてその妥当性を判定するための妥当性検査モジュールが提供される。ソフトウェア・オブジェクトのソース側は、少なくとも計算機ＩＤを入力として受け取り、一時キーを出力として生成する一時キー生成プログラムを保管している。インタフェース・プログラムはユーザ制御のデータ処理システムにロードされる。ユーザ制御のデータ処理システムの少なくとも１つの所定の属性を検査し、計算機ＩＤを生成するために、計算機ＩＤモジュールが使用される。この計算機ＩＤは、ソースとユーザとの対話時に不安定な通信チャネルを介してやりとりされる。ソフトウェア・オブジェクトのソース側では、一時キー生成プログラムへの入力として計算機ＩＤ（およびその他の情報）を使用して一時キーが生成される。この一時キーは、ソースとユーザとの対話時に、通常、不安定な通信チャネルを介してやりとりされる。次に、妥当性検査モジュールを使用して、一時キーの妥当性を判定する。その後、永続秘密キー生成プログラムを使用して、一時キーを受け取り、ソフトウェア・オブジェクトを暗号解読して一時的にそのオブジェクトへのアクセスを獲得するための永続秘密キーを生成する。一時キーによってソフトウェア・オブジェクトへの一時試用アクセスを可能にする一方で、分散データ処理システム内のある計算機から分散データ処理システム内の別の計算機へ暗号化ソフトウェア・オブジェクト、キー・ファイル、および計算機ＩＤファイルを転送するために携帯用メモリ媒体の使用を可能にするインポート・モジュールとエクスポート・モジュールもユーザに提供される。

【００１７】

【実施例】ソフトウェア製品の試用期間での使用を可能にするための本発明の方法および装置は、図１に示すようなスタンドアロン型ＰＣまたは図２に示すような分散データ処理システムで使用できる。いずれの場合にも、１つまたは複数のソフトウェア製品に対する一時試用期間アクセスは、特定のデータ処理システム属性を備えた特定のデータ処理システムにおける試用製品の使い方によって決まる。これは、１つまたは複数のデータ処理システム属性に基づく一時アクセス・キーを使用して試用ソフトウェア製品を暗号化することによって達成される。図３は、以下に詳述する一時アクセス・キーを作成する際に使用可能な複数のシステム構成属性を示したものである。まず、図１のスタンドアロン型データ処理システムの環境と、図２の分散データ処理システムについて詳しく説明し、次に、図３に示す特定のシステム構成属性について説明する。

【００１８】ここで添付図面、特に図１に関して説明すると、同図には、本発明によりプログラミング可能なデータ処理システム１０の絵画表現が示されている。図示の通り、データ処理システム１０は、好ましくはグラフィック・プロセッサと、メモリ装置と、中央処理装置（図示せず）とを含む、プロセッサ１２を含んでいる。このプロセッサ１２には、カラー・モニタまたはモノクロ・モニタのいずれかを使用して実現可能な表示装置１６が当技術分野で周知の方法で結合されている。また、プロセッサ１２にはキーボード１４も結合されている。キーボード１４は、ケーブルによってプロセッサに結合される標準のコンピュータ・キーボードで構成されるこ

とが好ましい。

【００１９】プロセッサ１２には、マウス２０などの図形ポインティング・デバイスも結合されている。このマウス２０は、ケーブルによって当技術分野で周知の方法でプロセッサ１２に結合されている。図示の通り、マウス２０は、左ボタン２４と右ボタン２６を含むことができ、そのそれぞれを押す、すなわち「クリック」すると、データ処理システム１０にコマンドおよび制御信号を出力することができる。開示されている本発明の実施例ではマウスを使用しているが、当業者は、本発明の方法を実施するためにライト・ペンまたはタッチ画面などの図形ポインティング・デバイスも使用できることに留意されたい。上記の説明を参照する際に、当業者は、ＩＢＭ製のモデル８０ＰＳ／２コンピュータなどのいわゆるパーソナル・コンピュータを使用してデータ処理システム１０を実現できることに留意されたい。

【００２０】本発明はスタンドアロン型データ処理システムで実施可能であるが、分散データ処理システムでも実施することができる。ただし、その場合は、分散データ処理システム内の特定のデータ処理装置間で携帯用メモリ媒体（ディスケットまたはテープなど）を介して１つまたは複数の暗号化ファイル、その暗号化キー・ファイル、および関連のファイル管理プログラムを転送するために、本発明のインポート・ルーチンとエクスポート・ルーチンが使用される。本発明のインポート・ルーチンおよびエクスポート・ルーチンについては後で詳述するが、基本的な分散データ処理システムについて説明し、これを理解しておくことが重要である。

【００２１】図３は、特定のデータ処理システム（スタンドアロン型か、分散データ処理システム内のノードか）を明確に識別するのに使用でき、さらに特定の定義済み試用期間の間、暗号化製品へのアクセスを獲得するのに使用できる一時アクセス製品キーを導出または生成する場合に使用する計算機ＩＤ値を生成するのに使用できる、複数のデータ処理システム属性を示すブロック図である。データ処理システムは、特定のシステム・バス６０アーキテクチャと、特定のメモリ制御装置７４と、バス制御装置７６と、割込み制御装置７８と、キーボード・マウス制御装置８０と、ＤＭＡ制御装置６６と、ＶＧＡビデオ制御装置８２と、並列制御装置８４と、直列制御装置８６と、ディスケット制御装置８８と、ディスク制御装置１０２とを含むことができる。さらに、特定のデータ処理システムを識別するために、複数の空または占有済みスロット１０６を使用することもできる。それぞれの特定のデータ処理システムは、ＲＡＭ７０、ＲＯＭ６８、またはＣＭＯＳＲＡＭ７２から導出可能な複数の属性を有することができる。計算機ＩＤ値を導出するために所定の方法で処理可能な、データ処理システムの１つまたは複数の属性を導出するために、プリンタ９６、モニタ９４、マウス９２、キーボード９０、ディスケット１００、またはディスク・ドライブ１０４などの端末装置を使用することもできる。この計算機ＩＤ値の導出については、後で詳述する。本発明は、ソフトウェア・プログラムのライセンスを（購入することによって）取得する前にそのプログラムを試すための手段をユーザに提供するために、ユーザにソフトウェア・プログラムを配布する効率の良い方法に関するものである。この概念により、ディスケットまたはＣＤ－ＲＯＭなどのコンピュータがアクセス可能なメモリ媒体に収めた完全なプログラムが潜在的ユーザに配布される。この概念は、ユーザが配布された媒体からプログラムにアクセスできるようにするためのキーを生成することにある。このような環境では、ユーザが各種ソフトウェア製品をブラウズできるようにする複数のインタフェースがファイル管理プログラムによって提供される。このインタフェースにより、配布された媒体に収容されたソフトウェア製品の注文とロック解除が可能になる。ソフトウェア製品のロック解除は、一時アクセス（暗号解読）キーの受取り、妥当性検査、および記録によって達成される。

【００２２】ファイル管理プログラムは、ユーザ制御のデータ処理システムに常駐し、ユーザのコンピュータ内でオペレーティング・システムの一部になる。（ＰＣＤＯＳ環境における）このような常駐プログラムの一例としては、ＤＯＳのファイル入出力操作を代行受信して処理する「終了後常駐」操作のための常駐プログラムＴＳＲが考えられる。ユーザに一時アクセス・キーが提供されると、このファイルが以前は試用動作モードで使用されていたかどうかを確認するため、システム・ファイルが検査される。製品を試用動作モードで使用したことがない場合は、一時キーが保管される。試用動作モード・キーが存在すると、ファイル管理プログラムによって開始された場合のみ、暗号化アプリケーションを実行することができる。この場合、ファイル管理プログラムは、アプリケーションが暗号化され、特定の操作用に有効な試用動作モード・キーが存在することを認識する。有効な試用動作モード・キーとは、期限が切れていないキーである。試用動作モードは、タイマまたはカウンタで定義することができる。すなわち、タイマを使用して特定の定義済み期間（たとえば、３０日）の秒読みを行うか、あるいはカウンタを使用して、試用動作モード中に許可される定義済み回数分の試用「セッション」の間、減分することができる。キーが有効な場合、ファイル管理プログラムは、ＴＳＲと直接やりとりし、特定の暗号化アプリケーションに関して試用動作モードを可能にする。その後、ファイル管理プログラムは暗号化アプリケーションを開始する。ユーザ制御のデータ処理システムのオペレーティング・システムに常駐するコードは、そのオペレーティング・システムに対する制御権を維持する。このコードは、ファイルを暗号解読してメモリにロードできるようにするために試用動作モード・キ

一の使い方を監視するが、暗号化ファイルが暗号解読されて媒体にコピーされるのを防止する。このような操作は、オペレーティング・システムを使用してどのアプリケーションがデータにアクセスしようとしているかを判定し、データへのアクセス許可を持っているアプリケーションだけ、アクセスできるようにすることで行われる。

【００２３】図４は、ソフトウェア・オブジェクトを暗号化するためのルーチンを示すブロック図である。ソフトウェア・オブジェクト２０１を構成する２進キャラクタは、暗号化エンジン２０５に入力として供給される。暗号化エンジン２０５では、暗号化キーとして実キー２０３が使用される。この暗号化エンジン２０５の出力は暗号化ソフトウェア・オブジェクト２０７になる。暗号化エンジン２０５は、公表され周知のＤＥＳアルゴリズムなどの従来の暗号化操作である場合もあれば、ソフトウェア・オブジェクト２０１を乱数化する排他的論理和演算であってもよい。

【００２４】図５は、本発明の教示によりソース２０９（ソフトウェア・ベンダ）とユーザ２１１（潜在的顧客）との間で行われる情報交換を示す絵画表現である。ソース２０９とユーザ２１１との間の矢印は、ベンダ２０９および２１１間で行われるオブジェクトまたは情報の交換を意味する。流れ２１３の交換では、コンピュータがアクセス可能なメモリ媒体がソース２０９からユーザ２１１に送られる。この転送は、郵便、宅配便、至急配達によって行われる場合もあれば、書籍や雑誌などの印刷物を介して引き渡される場合もある。あるいは、電子メールまたはその他の伝送技術を使用して、ソース２０９からユーザ２１１に電子文書が転送される場合もある。流れ２１５では、好ましくはユーザ２１１のデータ処理システムを識別する固有の計算機ＩＤ番号を含む、ユーザ固有情報が不安定な通信チャネルを介してユーザ２１１からソース２０９に転送される。通常、この情報は電話で交換されるが、電子メールまたはその他の通信技術を使用して渡される場合もある。流れ２１７では、ソース２０９がユーザ２１１に製品キーを提供する。この製品キーを使用すると、所定の定義済み期間の間、メモリ媒体に収容されている製品に一時的にアクセスできるようになる。この期間は、ユーザ２１１がそのソフトウェアに精通し、ソフトウェア製品を購入したいかどうかを決定できる「試用」期間と見なされる。ソフトウェア製品への永続アクセス権を取得するためには、ユーザ２１１はさらにソース２０９とやりとりしなければならない。製品キーによって、ユーザ２１１は特定の定義済み期間の間または特定の定義済み「セッション」数の間、そのソフトウェア製品へのアクセス権を取得することができる。時間の経過とともに、ユーザのクロックまたはカウンタの目盛りが減少する。試用期間が終了すると、それ以上アクセスしようとしても拒否される。このため、ユーザ２１１は、ソース２０９に連絡するとともに、ユーザ２１１に送られ、そのソフトウェア製品への無制限アクセスを可能にするために永続的に製品のロックを解除する永続キーを購入するための肯定的ステップを実行しなければならない。

【００２５】ソース２０９とユーザ２１１との間のやりとりはユーザ・インタフェースによって容易になる。このインタフェースの構築については図６の流れ図に示す。この処理は、ソフトウェア・ブロック２１９から始まり、ソフトウェア・ブロック２２１に続く。このブロック２２１では、ソフトウェア製品の試用期間中の使用の実現を容易にするインタフェースで使用される言語と通貨を決定するための言語および場所の選択がソース２０９によって行われる。複数のソフトウェア製品をひとまとめにし、コンピュータがアクセス可能な単一のメモリ媒体でユーザ２１１に配達する場合もある。このため、ソフトウェア・ブロック２２３により、ソース２０９は、コンピュータがアクセス可能なメモリ媒体上で試用に供されるプログラムに関する決定を行わなければならず、ソフトウェア・ブロック２２３により、該当するフィールドが記入される。次に、ソフトウェア・ブロック２２５により、プログラムが機能的に制限されるか、暗号化される。その後、ソフトウェア・ブロック２２７により、ディスケットまたはＣＤ－ＲＯＭなどのコンピュータがアクセス可能なメモリ媒体にコンピュータ・プログラム製品とともにシェル（ファイル管理プログラムを含みうる）がロードされる。この処理は、ソフトウェア・ブロック２２９で終了する。

【００２６】図７は、本発明によるベンダと顧客との対話を示す流れ図である。処理の流れは、ソフトウェア・ブロック２３１から始まり、ステップ２３３に続く。このステップ２３３では、試用／購入のための試用期間の間、コンピュータによりアクセス可能なメモリ媒体がユーザに配布される。その後、ステップ２３５により、コンピュータがアクセス可能なメモリ媒体からユーザ制御のデータ処理システムにファイル管理プログラムがロードされて実行される。このファイル管理プログラムは、ベンダと顧客との間の対話を容易にし、顧客が使用可能なオプションを示す、複数のインタフェース画面を含んでいる。このため、ステップ２３７により、ファイル管理プログラムが走査検索を可能にし、適切なユーザ・インタフェースを表示する。次に、ステップ２３９により、通常、電話または電子メールを介して顧客とベンダが対話し、ベンダが顧客に関する情報を収集して、定義済み試用期間の間、コンピュータがアクセス可能なメモリ媒体に収容されている１つまたは複数のソフトウェア製品へのアクセスを可能にする一時キーを配布できるようにする。一般に、この期間は、内部クロックか、または潜在的購入者が１つまたは複数の特定のソフトウェア製品に対して行うセッションの回数を追跡するカウンタ

によって定義される。ステップ２４１は、試用期間使用の許可を表している。その後、ソフトウェア・ブロック２４３により、ファイル管理プログラムは、データ処理システム内のすべての入出力呼出しを監視、監督し、コンピュータがアクセス可能なメモリ媒体に収容されている暗号化ソフトウェア製品の無許可使用を防止する。本発明の好ましい実施例のファイル管理プログラムは、暗号化ファイルへの呼出しを監視し、今後の処理のためにそのファイルが渡される前にアクセスを許可するか、拒否するかを決定する。このため、顧客は、ソフトウェア製品にアクセスして、それを購入するかどうかを決定することができる。その製品の購入を決定した場合は、ステップ２４５に示すように、顧客はもう一度ベンダと対話しなければならず、ベンダはその顧客に永続キーを引き渡さなければならない。顧客が永続キーを受け取り、購入した１つまたは複数のソフトウェア製品を暗号解読し、そのソフトウェア製品への通常の無制限アクセスが許可されると、処理が終了する。

【００２７】図８、図９、図１０、および図１１は、本発明による試用期間操作を容易にするユーザ・インタフェース画面を示している。図８は、顧客が別のウィンドウから「注文書表示」オプションを選択したときに表示される、注文書ユーザ・インタフェース２４９を示している。この注文書ユーザ・インタフェース２４９は、潜在的顧客とベンダとの対話を容易にするためにソフトウェア・ベンダを識別し、電話番号を提供する、タイトル・バー２５１を含んでいる。試用期間操作中に試すことができる１つまたは複数のソフトウェア製品を識別する注文書フィールド２５５が設けられている。また、数量サブフィールド２５９、品目サブフィールド２５７、説明サブフィールド２６０、および価格サブフィールド２５３を含む、複数のサブフィールドも設けられている。削除ボタン２６１を使用すると、潜在的顧客は注文書フィールドから品目を削除することができる。小計フィールド２６３は、注文したソフトウェアの価格の小計を示すものである。支払方法アイコン２６５は、可能な支払形式を識別する。当然のことながら、潜在的ユーザは、電話番号を使ってベンダに直接連絡して、１つまたは複数のソフトウェア製品を購入することができ、あるいは、妥当かどうか判断するためにソフトウェア製品を試す試用期間動作モード用として１つまたは複数のソフトウェア製品を選択することができる。注文書インタフェース２４９の最下部には、複数の機能アイコン２６７が設けられている。このようなアイコンとしては、クローズ・アイコン、ファックス・アイコン、メール・アイコン、印刷アイコン、ロック解除アイコン、ヘルプ・アイコンなどがある。ユーザは、従来のポイント・クリック操作で図形ポインティング・デバイスを使用し、これらの操作から１つまたは複数を選択することができる。ファックス・アイコンは、ファックス装置またはファックス・ボードを使用してベンダとの対話を容易にするものである。印刷アイコンは、ユーザがソフトウェア・ベンダとの対話を紙に印刷し、保存用コピーを作成できるようにするものである。

【００２８】顧客、コンピュータがアクセス可能なメモリ媒体、および顧客が使用するコンピュータ・システムは、媒体ＩＤ２６９、顧客ＩＤ２７３、および計算機ＩＤ２７１によって識別される。媒体ＩＤは、潜在的顧客に発送される前にコンピュータがアクセス可能なメモリ媒体に割り当てられている。このＩＤは固定されたものなので、変更できない。顧客ＩＤ２７３は、潜在的顧客とベンダとの対話から導出される。電話での対話中に選択した質問に顧客が回答し、特定の顧客に固有の顧客ＩＤ２７３をベンダが与える方法が好ましい。計算機ＩＤ２７１は、コンピュータがアクセス可能なメモリ媒体に常駐し、潜在的顧客が使用する特定のデータ処理システムに固有のファイル管理プログラムを使用して自動的に導出される。顧客は、通常、電話での対話によりベンダに計算機ＩＤを通知することになるが、ファックスでの対話や郵便での対話も可能である。

【００２９】図９は、注文情報ダイアログ・インタフェース２７５を示す図である。このインタフェースは、潜在的顧客を明確に識別する情報の獲得を容易にするもので、名前フィールド２７７、住所フィールド２７９、電話番号フィールド２８１、ファックス番号フィールド２８３、支払方法フィールド２８５、発送方法フィールド２８７、会員番号フィールド２８９、有効期限フィールド２９１、付加価値税ＩＤフィールド２９３を含んでいる。さらに注文情報ダイアログ・インタフェース２７５は、潜在的ユーザが上記の各種フィールドから情報を削除したり、インタフェース画面を紙面に印刷できるようにするための印刷ボタン２９５と取消しボタン２９７を含んでいる。

【００３０】図１０および図１１は、ロック解除ダイアログ・インタフェース画面３０１および３０３を示す図である。ユーザは、図形ポインティング・デバイスを使用して、ロック解除リスト３０５の構成要素である品目番号フィールド３０７および説明フィールド３０９によって識別される１つまたは複数の項目を選択する。このインタフェースはさらに、顧客ＩＤフィールド３１３と計算機ＩＤフィールド３１５を含んでいる。電話、ファックス、電子メールまたは郵便による対話でベンダが顧客に顧客ＩＤを与える方法が好ましい。また、ユーザは電話、ファックス、電子メールまたは郵便による対話中に計算機ＩＤフィールド３１５に計算機ＩＤを入力し、それをベンダに提供することが好ましい。試用期間操作中に要求される製品のＩＤとともにこの情報が交換されると、キー・フィールド３１１内に位置する一時アクセス・キーが提供される。このキーは、顧客が識別し選択した製品を一時的にロック解除するためのものである。

ユーザの対話を容易にするため、このインタフェース画面にはクローズ・ボタン３１９、保管ボタン３１７、およびヘルプ・ボタン３２１も設けられている。

【００３１】図１１は、単一製品ロック解除インタフェース画面３０３を示す図である。このインタフェース画面は、計算機ＩＤフィールド３１５、顧客ＩＤフィールド３１５、およびキー・フィールド３１１のみを含んでいる。このダイアログは単一製品のみに関するもので、しかも、一時試用期間操作が要求されている製品をユーザが知っているものと想定しているため、ロック解除する製品をこのインタフェースで識別するは必要ない。オペレータの対話を容易にするため、このインタフェースには保管ボタン３１７、取消しボタン３１９、およびヘルプ・ボタン３２１も設けられている。

【００３２】図１２は、試用期間動作モードを開始するために１つまたは複数の暗号化製品をロック解除する際に使用するユーザ・インタフェース画面を示している。図１０または図１１のいずれかのロック解除ダイアログで「保管」押しボタンを選択すると、図１２の開始日ダイアログが表示される。ここでユーザは、日付フィールド３１０に示されている正しい開始日を確認するよう要求される。ユーザは、「続行」ボタン３１２、「取消し」ボタン３１４、または「ヘルプ」ボタン３１６のいずれかをポイント・クリックすることで、この問合せに応答する。フィールド３１０に表示される日付は、ユーザ制御のデータ処理システムのシステム・クロックから導出される。この日付を試用期間操作の公式または指定開始日と対応させるために、ユーザがシステム・クロックを変更しなければならない場合もある。

【００３３】試用期間操作は２通りの形態が可能である。１つは、ユーザがすべての機能を試せるようにするが、データ・ファイルの印刷や保管などの重要機能は使用不可にするような、機能的に使用不可とする措置が施された製品である。もう１つの試用期間操作は、時間制限を設けて使用可能にした完全機能製品である。この場合はアクセス保護が必要であり、顧客は無料またはわずかな料金で製品のすべての機能を試すことができる。本発明によれば、通常、製品へのアクセスは「期限付き」キーによって制御される。製品を使用するための試用期間は、ベンダが決定した一定期間である。この試用期間はキーが発行されたときから始まる。本発明によれば、試用期間操作中に試用する製品は、顧客シェル内からしか実行できない。暗号解読ドライバは、暗号化製品の明文でのコピーを許可せず、顧客のシェルの外部での実行も許可しない。代替実施例では、顧客がその製品に対して実行する「セッション」ごとに増分または減分されるカウンタによって試用期間が定義される。この場合は、一時キーによる暗号解読が許可されなくなるまでに顧客は定義済み回数だけ製品を使用することができる。

【００３４】一時アクセス・キーの制限は、そのキーの「制御ベクトル」に組み込まれている。通常、制御ベクトルは、そのキーの簡単な説明、計算機ＩＤ番号、および試用期間データ（クロック値またはカウンタ値など）を含む定様式テキスト・ストリングを含む。キーを壊さずに制御ベクトルを変更することはできない。保護ソフトウェア製品を実行する場合は、操作試用期間の制限を実施するため、使用データを更新しなければならない。クロックまたはカウンタが不正操作されないように保護するため、その値は、通常は暗号化ファイル内の複数の場所に記録される。本発明の好ましい実施例では、試用期間情報（クロック値またはカウンタ値あるいはその両方）が「キー・ファイル」（後で詳述する）と、計算機ＩＤファイル（これについても後述する）と、システム・ファイルにコピーされる。暗号化プログラムへのアクセスが要求されると、上記の場所がすべて検査され、クロックまたはカウンタあるいはその両方の値が同じであるかどうか判定される。平均的なユーザが３つのファイルをすべて完璧に不正操作できるだけの高度の知識を持っている可能性は低い。好ましい実施例では、クロックとカウンタの組合せを使用して、バックアップの拡大使用と、システム・クロックをリセットするための回復操作を防止している。試用が要求されるたびにＰＣのクロックをリセットすることは可能であるが、これは、システム上の所与のファイルの日付／時間スタンプを追跡し、ファイルの日付／時間スタンプの中の最新の日付とシステム・クロックとを使用することで検出できる。前述の通り、タイマまたはカウンタあるいはその両方の情報が格納されている３つの場所の１つはシステム・ファイルである。オペレーティング・システムとしてＯＳ／２を使用して操作している場合、時間および使用データは、ＯＳ／２内のＯＳ２．ＩＮＩなどのシステム・データ・ファイルに格納することができる。試用および使用データをリセットするには、ユーザはこれらのファイルを連続バックアップし、回復しなければならなくなる。これらのファイルには、ユーザ・システムの動作にとって重要なその他のデータが収容されている。不用意なユーザがこれらのファイルを旧バージョンに回復しようとすると、他のアプリケーションにとって重要なデータを誤って紛失してしまう場合もある。本発明では、上記の保護技法により、不誠実なユーザが許可期間以上に試用期間使用を延長しようとする試みを確実に防止できる。

【００３５】大まかに概説すると、本発明では、ベンダがＣＤ－ＲＯＭまたは磁気媒体ディスケットなどのコンピュータがアクセス可能なメモリ媒体に複数の暗号化ソフトウェア製品をロードする。コンピュータがアクセス可能なメモリ媒体には、ソフトウェア・ベンダとソフトウェアの顧客との対話を容易にする複数のユーザ・インタフェース画面を提供する機能など、複数の機能を実行するファイル管理プログラムもロードされる。このコンピュータがアクセス可能なメモリ媒体はユーザ制御のデ

ータ処理システムに装填され、ファイル管理プログラムがロードされて実行される。ファイル管理プログラムは、顧客に関する情報（名前、住所、電話番号、および課金情報）を収集し、試用期間が要求されたソフトウェア製品に関する顧客の選択を受け取るための複数のユーザインタフェース画面を顧客に提供する。ソフトウェア・ベンダと顧客との間では、顧客ＩＤ番号、製品ＩＤ番号、媒体ＩＤ番号、および計算機ＩＤ番号などの情報が交換される。ベンダは、独自の内部記録に応じて顧客ＩＤ番号を生成する。ソフトウェアの潜在的顧客を識別するために、ソフトウェア・ベンダの担当者は顧客から情報を収集し、その情報を所定の用紙に記入しておくことが好ましい。あるいは、ソフトウェア・ベンダは、記入済みの注文情報ダイアログ・インタフェース画面２７５（図９）をファックス、電子メールまたは郵便で受け取ることもできる。配布されたメモリ媒体（ＣＤおよびディスケットなど）は、少なくとも一部がユーザ制御のデータ処理システムの１つの属性に基づく固有の計算機ＩＤを生成するためのファイル管理プログラムも含んでいる。この計算機ＩＤは、一度限りのセットアップ・プロセス中に作成される８ビットの乱数であることが好ましい。８つのランダム・ビットは、ルーチンの「種」としてシステム時間を使用する基本乱数発生ルーチンから生成されることが好ましい。また、最終結果には検査ビットが付加されていることが好ましい。注文を受け付ける人は電話を介して顧客が読み上げる計算機ＩＤをキー入力しなければならないので、この検査ビットは注文システムにとって重要である。この検査ビットを使用すると、顧客が番号を反復しなくても、計算機ＩＤを即時確認できる。ユーザ制御のデータ処理システムには、計算機ＩＤのクリア・テキスト（平文テキスト）と計算機ＩＤの暗号化バージョンを収容したマスタ・ファイルが保管されていることが好ましい。

【００３６】ソフトウェアの顧客は、ソフトウェア製品の一時試用に関する注文を行う場合、ソフトウェア・ベンダの電話受付に計算機ＩＤを口頭で伝える。それに対して、電話受付は、コンピュータがアクセス可能なメモリ媒体上の暗号化ソフトウェア製品に対する一時アクセス・キーとして機能する製品キーと、顧客ＩＤ番号とを顧客に伝える。この製品キーは、計算機ＩＤと、顧客番号と、注文されたプログラム用の実暗号化キーと、制御データ・ブロックとの関数であることが好ましい。ソフトウェアの顧客は、製品キーと顧客番号ならびに実暗号化キーを作成するための同一制御データ・ブロックを組み合わせることで製品キーを検査することができる。その後、このキーは、比較操作を可能にするために暗号化妥当性検査セグメントの暗号解読に使用される。暗号化妥当性検査セグメントが妥当性検査セグメント用の既知のクリア・テキストと同じであれば、ユーザのファイル管理プログラムは、その製品キーが正しい製品キーであり、ソフトウェア製品への一時アクセスに使用できると判断したことになる。このため、比較が一致すれば、そのキーはユーザ制御のデータ処理システムのキー・ファイルに格納される。このキー・ファイルには、製品キーと、顧客キー（顧客番号と内部キー生成キーに基づいて生成される）と、計算機ＩＤを含むクリアＡＳＣＩＩストリングとが収容されていることが好ましい。暗号解読ツールが実暗号化キーを導出できるようにするには、この３つの項目がすべてそのまま維持されている必要がある。さらにキー・ファイルをこの特定のユーザ制御のデータ処理システムに結びつけるため、システム・パラメータから導出されたキーを使って同じキー・ファイルが暗号化される。このようなシステム・パラメータは、データ処理システムの構成から導出することができる。

【００３７】大まかに説明すると、本発明の一時キー（通常は電話により口頭で伝えられる）は、暗号化を使用して実キーと、顧客番号、計算機ＩＤ番号、その他の定義済みクリア・テキストとを組み合わせるアルゴリズムによって作成される。したがって、このキーは１台の計算機だけに有効である。つまり、別の人にそのキーを伝えても、その人の計算機上のプログラムはロック解除されないはずである。このため、ソフトウェア・ベンダは、ライセンスによる収入を失うという重大な危険を冒さずに、ディスケットまたはＣＤ－ＲＯＭなどのコンピュータがアクセス可能なメモリ媒体で完全なプログラムを配布して、ソフトウェア・プログラムを販売することができる。

【００３８】暗号化操作に使用可能なシステムの好ましい固有属性としては、ハード・ディスクの製造番号、ハード・ディスクのサイズとフォーマット、システムの型式番号、ハードウェア・インタフェース・カード、ハードウェアの製造番号、その他の構成パラメータなどがある。この技法の結果、計算機ＩＤファイルは、ユーザ制御のデータ処理システムの同一クローンであるシステム上でしか暗号解読できなくなる。多くのデータ処理システムはそれぞれ構成が異なり、構成を一致させるにはかなり手間がかかるため、同一クローンを入手するのは非常に難しい。この点については、後で詳述する。

【００３９】次に図１３について説明すると、ファイル管理プログラムは、暗号化ソフトウェア製品とファイル管理プログラムがそこに収容された状態で配布された、コンピュータがアクセス可能なメモリ媒体を受け取る。ファイル管理プログラムは、図１３のステップ３５１に示すように、ユーザ制御のデータ処理システムの構成にアクセスする。ステップ３５３でデータ処理システムのユーザ固有属性が導出され、計算機ＩＤ生成プログラム３５５への入力として出力される。この計算機ＩＤ生成プログラムは、複数の２進文字を入力として受け取って、計算機ＩＤ３５７を表す擬似乱数出力を発生する、乱数発生ルーチン（乱数ジェネレータ）であることが好

ましい。計算機ＩＤ生成プログラム３５５が使用する処理は、複数の２進キャラクタを入力として受け取って、定義済みアルゴリズムにより複数の擬似乱数２進キャラクタを出力として発生する従来の擬似乱数発生ルーチンであればいずれでもよい。

【００４０】次に図１４に関して説明すると、計算機ＩＤ３５７は、暗号化形式でファイル管理プログラム内にも保管される。計算機ＩＤ３５７は、出力として暗号化計算機ＩＤ３６１を生成するために暗号化エンジン３５９に入力として供給される。暗号化エンジン３５９は、ＤＥＳアルゴリズムなどの規則暗号化ルーチンで構成することができる。暗号化エンジン３５９には入力としてキー３６３も供給され、このキー３６３が従来通り暗号化操作に作用する。キー３６３はシステム属性セレクタ３６５から導出される。選択候補となるタイプのシステム属性は、ハード・ディスクの製造番号、ハード・ディスクのサイズ、ハード・ディスクのフォーマット、システムの型式番号、ハードウェア・インタフェース・カード、ハードウェアの製造番号、その他の構成パラメータなどを含む、システム属性リスト３６７を含んでいる。

【００４１】本発明では、クリア・テキストの計算機ＩＤ３５７と暗号化計算機ＩＤ３６１がメモリに保管されている。また、本発明では、ファイル管理プログラムが適切なユーザ・インタフェース画面にクリア・テキストの計算機ＩＤ３５７を通知する。その後、ユーザは、図１５のブロック図によりその計算機ＩＤが使用されるソフトウェア・ベンダに計算機ＩＤを連絡する。図示の通り、製品キー暗号化エンジン３７５はソフトウェア・ベンダの制御下に維持される。この製品キー暗号化エンジン３７５は、計算機ＩＤ３５７と、顧客番号３６９（このソフトウェア・ベンダの内部記録機能により顧客に割り当てられているもの）と、実暗号化キー３７１（顧客の管理下にあるコンピュータがアクセス可能なメモリ媒体上に保管されたソフトウェア製品を暗号解読する場合に使用されるもの）と、制御ブロック・テキスト３７３（定義済みのテキスト部分とすることができる）と、試用期間データ３７４（試用期間を定義するクロック値またはカウンタ値など）とを入力として受け取る。製品キー暗号化エンジンは、製品キー３７７を出力として生成する。この製品キー３７７は、実キー３７１を暴露するという危険を冒さずに不安定な通信チャネルを介して顧客に伝えることができる。実キー３７１は暗号化操作によりマスキングされるが、製品キー３７７を使用できるのは計算機ＩＤ３５７が導出された構成と同一の構成を有するデータ処理システム上に限られるので、暗号化ソフトウェア製品へのアクセスは安全な状態で維持される。

【００４２】製品キー３７７が引き渡されると、ユーザ制御のデータ処理システムに常駐するファイル管理プログラムは、実キー生成プログラム３７９を使用して、製品キー３７７、顧客番号３６９、制御ブロック・テキスト３７３、計算機ＩＤ３５７、および試用期間データ３７４などの複数の入力を受け取る。実キー生成プログラム３７９は、導出された実キー３８１を出力として生成する。

【００４３】製品キー暗号化エンジン３７５（図１５）と実キー生成構成３７９（図１６）の動作を実行するのに使用する暗号化および暗号解読アルゴリズムについては、１９９２年１０月２１日に出願され、"Method and System for Multimedia Access Control Enablement"という名称の関連の米国特許出願第０７／９６４３２４号に記載されている。

【００４４】次に、図１７および図１８に示すように、ソフトウェア・ベンダによって提供された製品キー３７７の妥当性および信憑性を判定するため、導出された実キー３８１がテストされる。図示の通り、導出された実キー３８１は暗号化エンジン３８５に一方の入力として供給される。この暗号化エンジン３８５へのもう一方の入力として、所定の暗号化妥当性検査データ・セグメント３８３が供給される。暗号化エンジンは、導出されたクリア妥当性検査テキスト３８７を出力として供給する。その後、図１８により、導出されたクリア妥当性検査テキスト３８７が比較器３８９で既知のクリア妥当性検査テキスト３９１と比較される。この比較器３８９は、導出されたクリア妥当性検査テキスト３８７と既知のクリア妥当性検査テキスト３９１との比較をビットごとに行うだけである。導出されたクリア妥当性検査テキスト３８７が既知のクリア妥当性検査テキスト３９１と一致すると、ステップ３９３によりキー・ファイルが作成されるが、導出されたクリア妥当性検査テキスト３８７が既知のクリア妥当性検査テキスト３９１と一致しない場合は、ステップ３９５によりユーザ制御のデータ処理システムに警告が通知される。

【００４５】次に図１９に移って説明すると、キー・ファイル３９７は、一時製品キー、顧客キー（顧客番号の暗号化バージョン）、クリア・テキストでの計算機ＩＤ番号、および試用期間データ（クロック値またはカウンタ値など）を含むものとして示されている。このキー・ファイルは、暗号化エンジン３９９に入力として供給される。暗号化エンジン３９９には、キー４０１も入力として供給される。キー４０１は、計算機ＩＤ番号を導出する際に使用するシステム属性のような固有のシステム属性４０３から導出される。暗号化エンジン３９９は、暗号化キー・ファイル４０５を出力として提供する。

【００４６】図２０、図２１、図２２、図２３、および図２４は、一時アクセスキーが受け取られ、妥当性が検査され、キー・ファイル３９７（図１９）に記録された後で行われるファイル管理プログラムの操作を示している。

【００４７】図２０は、暗号化ソフトウェア製品が処理

のためにユーザ制御のデータ処理システムによって呼び出されたときに実行される各種ステップを示すブロック図である。まず、暗号化ファイル４０５が取り出され、「ヘッダ」部４０７がユーザ制御のデータ処理システムによって読み取られる。このヘッダは、キー・ファイルの位置を含む複数の構成要素を有する。キー・ファイルの位置は、ステップ４０９によりキー・ファイルを取り出すために使用される。さらにヘッダは、暗号化妥当性検査テキスト４１１も含んでいる。この暗号化妥当性検査テキスト４１１もユーザ制御のデータ処理システムによって読み取られる。前述の通り（および図１９に示す通り）、キー・ファイルは製品キー４１９、顧客キー４１７、および計算機ＩＤ４１５を含んでいる。図２１に示すように、これらは暗号解読エンジン４１３に入力として与えられる。暗号解読エンジン４１３は、出力として実キー４２１を提供する。実キー４２１を使用して配布されたメモリ媒体上の暗号化ソフトウェア製品を暗号解読する前に、妥当性を判定するためにこの実キーがテストされる。図２２は、妥当性検査テストのブロック図である。「ヘッダ」に収容されている暗号化妥当性検査テキスト４２３は、入力として暗号解読エンジン４２５に供給される。この暗号解読エンジン４２５には、実キー４２１（図２１の操作で導出されたもの）も入力として供給される。暗号解読エンジン４２５は出力としてクリア妥当性検査テキスト４２７を提供する。図２３のブロック図に示すように、クリア妥当性検査テキスト４２７が入力として比較器４２９に供給される。この比較器４２９には、既知のクリア妥当性検査テキスト４３１も入力として供給される。比較器４２９は、導出されたクリア妥当性検査テキスト４２７が既知のクリア妥当性検査テキスト４３１と一致するかどうかを判定する。テキスト同士が一致すると、ステップ４３３によりソフトウェア・オブジェクトが暗号解読されるが、妥当性検査テキスト部同士が一致しない場合は、ステップ４３５により警告が通知される。図２４は、図２３のステップ４３３の暗号解読操作を示すブロック図である。まず、暗号化ソフトウェア・オブジェクト４３７が入力として暗号解読エンジン４３９に与えられる。この暗号解読エンジン４３９には、妥当性検査された実キー４４１も入力として供給される。暗号解読エンジン４３９は、出力として暗号解読したソフトウェア・オブジェクト４４３を供給する。

【００４８】暗号化ヘッダは、あるファイルがクリアテキスト・ファイルとともに格納されたときにそのファイルが暗号化されているかどうかの判定に対応するために設けられている。導入時の妥当性検査ステップ（本発明の概念とは一切無関係である）の一部としてファイル・サイズを検査する場合があるので、暗号化ファイルに暗号化ヘッダを設ける際に、ファイル・サイズを変更しないことが重要である。このため、そのファイルのサイズを想定以上にすると、ソフトウェアの導入時に操作上の困難が発生する場合がある。暗号化製品にアクセスする可能性のある他のソフトウェア・アプリケーションは元のファイル名を使用してそのファイルにアクセスするので、ファイルが暗号化されているという事実を反映するために暗号化ソフトウェア製品に関連するファイル名を変更することができず、そのため、暗号化ヘッダの必要性がさらに増すことになる。したがって、ファイルが暗号化されていることを示すためにファイル名を変更すると、暗号化ソフトウェア製品と他のおそらく関連あるソフトウェア製品との有益かつ望ましいやりとりが阻害される恐れがある。たとえば、表計算アプリケーションでは、通常、印刷文書に財務情報を統合できるようにするために関連のワード・プロセッサ・プログラムに表計算の各部を移植することができる。ワード・プロセッサ・プログラム用のハードコード化された元のファイル名を変更すると、これらのソフトウェア製品間の有益なやりとりが阻害される恐れがある。本発明の暗号化ヘッダは、暗号化ファイルをその名前ファイル長で保管し、ソフトウェア製品用のファイル名を未変更の形式で保管することで、上記の問題を解決するものである。

【００４９】図２５は、暗号化ヘッダ４５１を備えた暗号化ファイルを示す図である。暗号化ヘッダ４５１は、固有のＩＤ部４５３、キー・ファイル部の名前４５５、暗号化妥当性検査セグメント４５７、暗号化タイプ４５９、サイド・ファイルへのオフセット４６１、暗号化ファイル・データ４６３などを含む複数のコード・セグメントを含んでいる。当然のことながら、この図の暗号化ファイル・データ４６３は、ワード・プロセッサ・プログラムまたは表計算などの暗号化ソフトウェア製品を表している。暗号化ヘッダ４５１は、通常は暗号化ソフトウェア製品の一部を構成するはずの暗号化データの代わりに提供される。また、暗号化ヘッダは、暗号化ソフトウェア製品の最初の部分の位置に代入される。暗号化ファイル・データ４６３からなる暗号化ソフトウェア製品の前面に暗号化ヘッダ４５１を配置するためには、暗号化ファイル・データの一部を別の場所にコピーしなければならない。サイド・ファイルへのオフセット４６１は、移動されたファイル・データが収容されているサイド・ファイル位置を識別するものである。

【００５０】図２６は、暗号化ファイルのディレクトリとサイド・ファイルとの関係を示す図である。図示の通り、暗号化ファイルのディレクトリ４６５は、ファイルａａａ、ファイルｂｂｂ、ファイルｃｃｃ、ファイルｄｄｄからファイルｎｎｎまでを含んでいる。これらのファイルのそれぞれは、特定の暗号化ソフトウェア製品のディレクトリ名を表している。各暗号化ソフトウェア製品には、ファイルのサイズとファイル名を変更せずに暗号化ヘッダ４５１を収容するために移動されたファイルの前面部分が入っているサイド・ファイルが関連付けら

れている。ファイルａａａにはサイド・ファイルＡＡＡが関連付けられている。ソフトウェア製品ファイルｂｂｂにはサイド・ファイルＢＢＢが関連付けられている。暗号化ソフトウェア製品ｃｃｃにはサイド・ファイルＣＣＣが関連付けられている。暗号化ソフトウェア製品ｄｄｄにはサイド・ファイルＤＤＤが関連付けられている。暗号化ソフトウェア製品ｎｎｎにはサイド・ファイルＮＮＮが関連付けられている。図２６のディレクトリ名４６７、４６９、４７１、４７３、４７５は、サイド・ファイル４７７、４７９、４８１、４８３、４８５に関連するものとして示されている。このサイド・ファイルの目的は、ファイル・サイズを変更せずに暗号化ソフトウェア製品のそれぞれに暗号化ヘッダでタグを付けられるようにすることにある。

【００５１】暗号化ヘッダ４５１の暗号化タイプ・セグメント４５９は、暗号化ソフトウェア製品の暗号化に使用される暗号化のタイプを識別するものである。製品の暗号化にはいくつかある従来の暗号化技法のいずれも使用可能であり、同一メモリ媒体上に収容されている複数の異なるソフトウェア製品を暗号化する場合は異なる暗号化タイプを使用することができる。このため、暗号化タイプ・セグメント４５９により、暗号化ソフトウェア製品を暗号解読するために適切な暗号化／暗号解読ルーチンが確実に呼び出される。ただし、この場合、一時アクセス・キーが有効で期限切れになっていないことが条件となる。暗号化ヘッダ４５１のキー・ファイル・セグメントの名前４５５は、キー・ファイルのアドレス（通常、ディスク・ドライブ位置）を提供する。（図１９に関連して）前述の通り、キー・ファイルは、製品キー、顧客キー、およびクリア計算機ＩＤを含んでいる。（図２１により）実キーを生成するには、これらの３つの情報がすべて必要になる。暗号化妥当性検査セグメント４５７は、図２３のルーチンを使用して既知のクリア妥当性検査テキストとの比較が可能な導出済みクリア妥当性検査テキストを生成するための図２２に示すルーチンで使用される暗号化妥当性検査テキストを含んでいる。導出されたクリア妥当性検査テキストが既知のクリア妥当性検査テキストと完全に一致する場合のみ、導出され妥当性検査された実キーを使用して図２４により暗号化ソフトウェア製品を暗号解読することにより、処理を続行することができる。しかし、図２４の暗号解読操作を実行する前に、暗号化ヘッダ４５１の代わりに対応するサイド・ファイルの内容を暗号化ソフトウェア製品に戻しておかなければならない。これにより、暗号解読操作の前に暗号化ソフトウェア製品が完全なものになる。

【００５２】ユーザ制御のデータ処理システムのオペレーティング・システムによる処理のためにファイルが呼び出されるたびに、そのオペレーティング・システムに常駐するファイル管理プログラムが入出力要求を代行受信（intercept）し、ファイルの前面部分を検査して、固有のＩＤ４５３のような暗号解読ブロックＩＤが特定の既知の場所に存在するかどうかを判定する。パフォーマンスを最善にするため、図２５に示すように、通常、この場所はファイルの先頭になる。ファイルが暗号解読ブロックを備えているとファイル管理プログラムが判定すると、ＴＳＲ（終了後常駐もしくは常駐終了型プログラム）がそのブロックをメモリに読み込む。その後、キー・ファイルが入っているドライブおよびディレクトリを指定する環境変数をコピーし、暗号化ブロックからのキー・ファイル名を連結することで完全修飾キー・ファイル名を作成するために、その暗号解読ブロックが解析される。次に、ＴＳＲはキー・ファイルのオープンを試みる。キー・ファイルが存在しない場合は、ＴＳＲは、暗号化ファイルのオープンを試みているアプリケーションに「アクセス拒否」応答を返す。キー・ファイルが存在すると判定された場合は、ＴＳＲはキー・ファイルをオープンし、各種のキー（製品キー、顧客キー、および計算機ＩＤ）を読み込んで、実キーを生成する。この実キーは、暗号解読ブロック妥当性検査データを暗号解読するために使用されている。前述の通り、比較操作によって、この暗号解読操作が正常に行われたかどうかが判定される。比較が失敗に終わった場合、キー・ファイルは「無効」であると判定され、暗号化ソフトウェア製品のオープンを試みているアプリケーションに対してＴＳＲが「アクセス拒否メッセージ」を返す。しかし、比較が正常に行われた場合は、ファイル管理プログラムは、暗号化ヘッダで検出された暗号化タイプに応じてファイルの暗号解読の準備を行う。その後、ファイルがオープンされたことを示すために、ＴＳＲは有効なファイル・ハンドルを呼出し側アプリケーションに返す。アプリケーションが暗号化ファイルからデータを読み取る場合、ＴＳＲは、アプリケーションに戻す前にこのデータを読み取って暗号解読する。要求されたデータがサイド・ファイル内に格納されている移動済みデータの一部である場合は、データが別のファイルからのものであることを呼出し側アプリケーションに知らせずに、ＴＳＲがサイド・ファイルを読み取って、適切な暗号解読済みブロックを呼出し側アプリケーションに返す。

【００５３】図２５および図２６では暗号化ヘッダの大まかな概念を示したが、図２７、図２８、および図２９では暗号化ファイルの作成に関するより詳細な態様を示す。図２８および図２９は、２種類のデータ・ファイルを示している。図２８は非実行データ・ファイルを示しているのに対し、図２９は実行データ・ファイルを示している。また、図２７は、シグナチャ・セグメント５０１、ヘッダＬＥＮ５０３、サイド・ファイル・インデックス５０５、サイド・ファイルＬＥＮ５０７、暗号解読タイプＩＤ５０９、検証データ５１１、およびキー・フィル名５１８を含むヘッダ４９９を示している。図２８に示すように、ソフトウェア製品はクリア・ファイル５

２１として始まり、特定の暗号化ルーチンにより暗号化ファイル５２３に暗号化される。クリア・ファイル５２１を暗号化ファイル５２３に変更する場合に使用される暗号化のタイプは、ヘッダ４９９の暗号化タイプ・セグメント５０９によって識別される。次に、暗号化ファイル５２３の前面部分が、ヘッダ４９９のサイド・ファイル・インデックス５０５とサイド・ファイルＬＥＮ５０７によって識別されるサイド・ファイル５２７にコピーされる。さらに、サイド・ファイル５２７には、検証データのクリア・テキストのコピーも含まれる。その後、修正済み暗号化ファイル５２５を形成するためにヘッダ４９９が暗号化ファイル５２３の前面部分にコピーされる。図２９に示すように、実行ファイルについても同様の処理が行われる。暗号化ファイル５３３を形成するために、ソフトウェア製品のクリア・テキスト・コピー（クリア・ファイル５３１として表されているもの）が従来のルーチンにより暗号化される。暗号化ファイル５３３のデータの重なり（オーバレイ）が防止されるように、暗号化ファイル５３３の前面部分がサイド・ファイル５３９にコピーされる。しかも、サイド・ファイル５３９は、検証データのクリア・テキストのコピーを含む。その後、暗号化ファイル５５３の最初の部分（前面部分）に実行可能スタブ５３７とヘッダ５９９をオーバレイすることで、暗号化ファイル５３３が修正される。

【００５４】ここで図２９の実行可能スタブ５３７の目的について説明する。パーソナル・コンピュータ用のＤＯＳオペレーティング・システムは、暗号化アプリケーションの実行を試みる。その結果、システムが「ハング」したり、好ましくないアクションを起こす場合がある。図２９の実行ファイルの実行可能スタブ５３７は、暗号化されたアプリケーションの実行をユーザが試みないようにするために使用される。つまり、ユーザが暗号化ファイルを実行しようとすると、システムをハングさせたり、ドライブをフォーマットしたりする危険性がかなり大きいと思われる。導入済みＴＳＲを使用せずにアプリケーションを実行したり、ＴＳＲが「監視」していないドライブからアプリケーションを実行した場合に必ず実行可能スタブが実行されるように、このスタブは暗号化ソフトウェア製品の前面部分に接続されている。このスタブによって、アプリケーションを実行できない理由を説明するメッセージがユーザに通知される。この実行可能スタブを使用すると、メッセージの提供以外に、次のような高度なアクションを実行することができる。

（１）ＴＳＲの機能性を複写し、もう一度アプリケーションを開始する前に動的暗号化を導入することができる。

（２）一時アクセス・キーをオンにして、もう一度アプリケーションを開始することができる。

（３）ＴＳＲとやりとりして、アプリケーションの実行元であるドライブを調べるよう通知することができる。

【００５５】実行可能スタブは、暗号化プログラムに次のように保管またはコピーされる。

（１）アプリケーションを暗号化する。

（２）このプログラム用に暗号解読ブロックを作成する。

（３）暗号解読ブロックの前面部分に事前作成実行可能スタブが接続される。

（４）結合した暗号解読ヘッダと実行可能スタブの長さを求める。

（５）実行可能ファイルの前面にあってこの長さに匹敵するバイト数がメモリ、好ましくは定義済みのサイド・ファイル位置に読み込まれる。

（６）暗号化ヘッダと実行可能スタブが実行可能コードの先行バイトの上に上書きされる。

【００５６】ＴＳＲは、実行可能スタブの「既知のサイズ」を超えて暗号解読ブロック部分を探索することで、実行可能スタブが暗号化されているかどうかを判定できる。ＴＳＲは、実行可能スタブを暗号解読するときに、サイド・ファイルにアクセスし、スタブとヘッダ・ブロックによって移動されたバイトを読み込む。

【００５７】図３０および図３１は、試用期間中の操作を示す流れ図であり、この操作はソフトウェア・ブロック６０１から始まる。ソフトウェア・ブロック６０３により、ユーザ制御のデータ処理システムのオペレーティング・システム内に位置するファイル管理プログラムがメモリ媒体への入出力呼出しを連続監視する。その後、ソフトウェア・ブロック６０５により、各入出力呼出しごとに被呼ファイルがファイル管理プログラムにより代行受信され、ソフトウェア・ブロック６０７により、アクセスを許可すべきかどうかをファイル管理プログラムが判定できるようになるまで、オペレーティング・システムから被呼ファイルへのアクセスが拒否される。被呼ファイルのうち、暗号解読ブロックが位置するはずの部分が読み取られる。その後、ソフトウェア・ブロック６０９により、被呼ファイルのこの部分が読み出され、ソフトウェア・ブロック６１１により、キー・ファイル・アドレスが導出される。導出されたアドレスは、ソフトウェア・ブロック６１３によりキー・ファイルを取り出す際に使用される。判定ブロック６１５の結果、キー・ファイルを突き止められない場合は、ソフトウェア・ブロック６１７で処理が終了する。しかし、判定ブロック６１５により、キー・ファイルを突き止めることができると判定された場合は、ソフトウェア・ブロック６１９によりキーが導出される。その後、ソフトウェア・ブロック６２１により、導出されたキーを使用して、暗号化ヘッダ内に位置する妥当性検査セグメントが暗号解読される。判定ブロック６２３では、暗号解読妥当性検査セグメントが暗号解読妥当性検査セグメント用のクリア・テキストと比較される。暗号解読されたセグメントが既知のクリア・テキスト・セグメントと一致しない場合

は、処理はソフトウェア・ブロック６２５に続き、終了する。しかし、判定ブロック６２３で、暗号解読された妥当性検査セグメントが既知のクリア・テキスト妥当性検査セグメントと一致すると判定されると、処理はソフトウェア・ブロック６２７に続き、そこで被呼ファイルへのアクセスが許可される。次に、ソフトウェア・ブロック６２９により、暗号解読ヘッダから暗号解読タイプが読み取られ、ソフトウェア・ブロック６３３によりユーザ制御のデータ処理システムのオペレーティング・システムによる処理のために渡されたときに、被呼ファイルがソフトウェア・ブロック６３１により動的に暗号解読される。処理はソフトウェア・ブロック６３５で終了する。

【００５８】暗号化ファイルの無許可実行を試みると、実行可能スタブは少なくとも一時的にアクセスを拒否し、システムにメッセージを通知するが、前に列挙したいくつかの高度な方法で問題を処理することができる。

【００５９】本発明の好ましい実施例によれば、見込みのある購入者は、試用期間中または試用期間終了時に、コンピュータがアクセス可能なメモリ媒体上の１つまたは複数のソフトウェア製品のコピーの購入準備のためにベンダに連絡する可能性がある。潜在的ユーザに製品を発送するためにＣＤ－ＲＯＭまたはフロッピー・ディスクが使用されていることが好ましい。また、コンピュータがアクセス可能なメモリ媒体は、試用期間用に提供される各製品について暗号化したコピーを２つ含むことが好ましい。一方の暗号化コピーは、ファイル管理プログラムと、ベンダから購入者に通知される一時キーとを使用して暗号解読することができる一次的なものである。もう一方の暗号化コピーは、試用期間動作モードでの使用を目的として提供されるのではなく、ソフトウェア製品の購入後に暗号解読と使用が可能になる永続コピーとして提供されるものである。大まかに概説すると、ユーザは、試用期間動作モード用にソフトウェア製品を選択し、（ファイル管理プログラムにより）定義済み試用期間中の製品へのユーザ・アクセスを可能にする一時アクセス・キーをベンダから取得する。試用期間終了前または終了後にユーザは、ファックス、電子メール、または電話によってベンダに連絡することで、ソフトウェア製品の永続コピーをベンダから購入することができる。支払を受け取ると、ベンダは、ソフトウェア製品のもう１つの暗号化コピーを暗号解読するのに使用する永続アクセス・キーをユーザに通知する。この暗号化製品は、ＤＥＳアルゴリズムなどの従来の暗号化ルーチンを使用して暗号化することができる。永続キーにより、ソフトウェア製品を暗号解読して無制限に使用することができる。１回のトランザクションで１つの製品の複数のコピーを購入する場合があるため、本発明は、可動アクセス・キーを提供するための技法を備えている。この可動アクセス・キーについては、図３２～図３７に関連して後述する。本発明の好ましい実施例で使用するソフトウェア製品の上述の第２のコピーを暗号化し暗号解読するための暗号化アルゴリズムは、試用期間動作モードで使用するものと同様である。

【００６０】本発明は、試用期間終了後に永続アクセス・キーの配布に対応するためのエクスポート（送信）／インポート（受信）機能を含んでいる。通常、オフィスの管理者またはデータ処理システムの管理者は、試用期間終了後に暗号化製品の指定数の複数の「コピー」を購入する。その後、組織内の所与の個人に対し、暗号化製品への無制限かつ永続的なアクセスを可能にする永続キーが発行される。分散データ処理ネットワーク内に計算装置が接続されていないオフィスや作業環境では、オフィスの管理者またはデータ処理システムの管理者から、組織内で暗号化ソフトウェア製品のコピーの受取りが予定されている指定の個人に対し、永続アクセス・キーを通知しなければならない。永続キーは製品への永続的アクセスに対応するものである。特定の暗号化製品のコピーを組織内のすべての従業員に発行できるわけではないので、ベンダとしては、売買契約またはライセンス契約を超えるような配布を最小限に抑えるか防止するような配布方法を希望するはずである。製品は暗号化されているため、暗号化した形式であれば自由に配布することができる。本発明で保護の対象となるのは、製品への無制限アクセスを可能にする各種キーである。電子メールや印刷物のやりとりでキーが配布されるのを防止するため、本発明は、ソース・コンピュータに常駐するエクスポート・プログラムと、ターゲット・コンピュータに常駐するインポート・プログラムとを含み、これらのプログラムにより、フロッピー・ディスクなどの取外し可能メモリ媒体を介して行われるアクセス・キーの配布に対応している。このため、アクセス・キーが不注意や事故によって配布または開示されることはなくなる。この目標を達成するための主な実施例は２通りある。

【００６１】第一の実施例では、ソース・コンピュータに保管されている１つまたは複数の暗号化ファイルがまず暗号解読され、次に暗号化アルゴリズムと移送可能メモリ媒体に固有の暗号化キー（ディスケットの製造番号など）を使用して、そのファイルが暗号化される。キー・ファイルはディスケットによってターゲット・コンピュータに物理的に運搬することができ、そのターゲット・コンピュータでは転送可能メモリ媒体との対話によりターゲット・コンピュータが導出したキーを使用してキー・ファイルの暗号解読が行われる。その後直ちに、ターゲット・コンピュータの固有のシステム属性から導出されたキーで鍵がかけられた暗号化操作を使用して、キー・ファイル（複数も可）の暗号化が行われる。

【００６２】第二の実施例では、ターゲット・コンピュータに明確に関連付けられ、ターゲット・コンピュータの１つまたは複数の固有のシステム属性から導出可能な

転送キーをターゲット・コンピュータのインポート・ファイルから獲得するために、転送可能メモリ媒体がターゲット・コンピュータに装填される。その後、メモリ媒体はソース・コンピュータに転送され、そこで１つまたは複数のキー・ファイルが暗号解読され、さらに転送キーを使用して暗号化される。次に、メモリ媒体はターゲット・コンピュータに運搬され、そこで転送キーが生成され、１つまたは複数のキー・ファイルを暗号解読するための暗号解読操作で転送キーが使用される。ターゲット・コンピュータに明確に関連付けられ、１つまたは複数の固有のコンピュータ構成属性から導出可能なキーで鍵がかけられた暗号化操作を使用して、直ちにキー・ファイルの暗号化が行われることが好ましい。第一の実施例については、図３２、図３３、図３４、および図３５に関連して説明する。また、第二の実施例については、図３６および図３７に関連して説明する。

【００６３】図３２および図３３は、別のシステムへのインポートが可能になっているアクセス・キーの固有のディスケット・イメージを生成する「エクスポート」機構を使用して、許可ユーザが永続キーを別のデータ処理システムへ移動できるようにするためのエクスポート操作とインポート操作をブロック図形式で示したものである。本発明によれば、ソフトウェア・ベンダから顧客に電話で引き渡されるアクセス・キーの長さは４０バイト未満である。生成されたキー・ファイルの長さは２０００バイトを上回る。キー・ファイルと計算機ＩＤファイルをディスケットにコピーするためのエクスポート機構が設けられている。誰でも使用可能な公共フォーラムにコピーされるのを禁止するために、両方のファイルは、修正済みのディスケット製造番号で暗号化される。別のシステムに設けられているインポート機構は、これらのファイルを暗号解読し、ディスケットから得た製品キーと計算機ＩＤをインポート・システム・マスタ・ファイル内のインポート製品キーおよび計算機ＩＤのリストに追加し、そのキー・ファイルをインポート・システム・ハード・ディスクにコピーする。前に開示したとおり、このキー・ファイルがインポート・システム上で暗号化される。

【００６４】図３２は、本発明の好ましい実施例によるエクスポート操作を示すブロック図である。図示の通り、ソース・コンピュータ６５１は、キー・ファイル６５３と計算機ＩＤファイル６５５とを含む。キー・ファイル６５３は、製品キーと、顧客キーと、ソース・コンピュータ６５１用の計算機ＩＤのクリア・テキストと、試用期間データ（試用期間を定義するクロックまたはカウンタあるいはその両方など）と、特定の保護ソフトウェア製品について許可されたエクスポート操作の最大数を定義し、実施されたエクスポート操作の総数を追跡するという二重機能を実行するエクスポート・カウンタとを含む。計算機ＩＤファイルは、計算機ＩＤ番号と試用期間データ（試用期間を定義するクロックまたはカウンタあるいはその両方など）とを含む。キー・ファイル６５３と計算機ＩＤファイル６５５はどちらも従来の暗号化操作（ＤＥＳアルゴリズムなど）によって暗号化されるが、この操作はソース・コンピュータ６５１の固有のシステム属性から導出されるキーで鍵がかけられている。エクスポート操作の開始時に、キー・ファイル６５３と計算機ＩＤファイル６５５が暗号解読される。キー・ファイル６５３は、キー６５９で鍵がかけられた暗号解読操作６５７に入力として供給される。同様に、計算機ＩＤファイル６５５は、キー６６１で鍵がかけられた暗号解読操作６６３に入力として供給される。暗号解読操作６５７および６６３は、キー・ファイル６５３と計算機ＩＤファイル６５５のクリア・テキスト・バージョンを生成する。クリア・テキストが得られると、キー・ファイル６５３内に収容されているエクスポート・カウンタがブロック６６１により修正される。たとえば、この操作が、許される１０回の操作のうちの７回目のエクスポート操作であれば、カウンタは”７：１０”と表示するはずである。キー・ファイル６５３のクリア・テキスト・バージョンは暗号化操作６６９に入力として供給される。この暗号化操作６６９は、従来のいずれの暗号化操作（ＤＥＳアルゴリズムなど）でもよく、修飾子６６７による修正の対象となったソース・コンピュータ６５１に結合されたメモリ媒体に固有のメモリ媒体属性６６５で鍵がかけられる。たとえば、メモリ媒体６７７に固有の「メモリ媒体属性」として固有のディスケット製造番号を供給することができる。わずかに変更して暗号化操作６６９に入力として供給するために、ディスケット製造番号は修飾子６６７により修正される。計算機ＩＤファイル６５５のクリア・テキストについても同じ操作が行われる。すなわち、固有のメモリ媒体属性６７１が修飾子６７３によって修正され、暗号化操作６７５のキーとして使用される。この暗号化操作は、ＤＥＳ操作などの従来の暗号化操作で構成することができる。最後に、暗号化操作６６９および６７５の出力がコピー操作６７９および６８１に入力として供給され、暗号化キー・ファイル６５３と計算機ＩＤファイル６５５がメモリ媒体６７７にコピーされる。

【００６５】図３３は、インポート操作を示すブロック図である。メモリ媒体６７７（図３２）はソース・コンピュータ６５１（図３２）から物理的に取り外され、コンピュータ７０７（図３３）に物理的に運搬される。あるいは、分散データ処理システムではこの転送は、メモリ媒体６７７の物理的な取外しを伴わずに行われる場合もある。ここで図３３に関して説明すると、どの特定のターゲット・コンピュータがキー・ファイルと計算機ＩＤファイルを受け取ったかを記録するために、ブロック６８３により、ターゲット・コンピュータの計算機ＩＤがメモリ媒体６７７にコピーされる。次に、ブロック６

８５および６９３により、暗号化キー・ファイル６５３と計算機ＩＤファイル６５５がメモリ媒体からターゲット・コンピュータ７０７にコピーされる。暗号化キー・ファイル６５３は、キー６８７で鍵がかけられた暗号解読操作６８９に入力として供給される。暗号解読操作６８９は、ブロック６６９の暗号化操作を取り消すもので、キー・ファイル６５３のクリア・テキスト・バージョンを出力として提供する。同様に、計算機ＩＤファイル６５５は、キー６９５で鍵がかけられた暗号解読操作６９７に入力として供給される。暗号解読操作６９７は、暗号化操作６７５の暗号化を取り消すもので、計算機ＩＤファイル６５５のクリア・テキストを出力として提供する。ブロック６９１により、ソース・コンピュータ６５１の計算機ＩＤが取り出され、キー・ファイル６５３のクリア・テキストとしてメモリ内に記録される。次に、キー・ファイル６５３のクリア・テキストが暗号化操作６９９に入力として供給される。暗号化操作６９９は、ＤＥＳ操作などの従来の暗号化操作であり、ターゲット・コンピュータ７０７用の計算機ＩＤまたは修正済み計算機ＩＤなどのターゲット・コンピュータ固有の属性で鍵がかけられている。計算機ＩＤファイル６５５のクリア・テキストは、暗号化操作７０３に入力として供給される。この暗号化操作７０３は、ＤＥＳ暗号化操作などの従来の暗号化操作であり、ターゲット・コンピュータ７０７の計算機ＩＤまたは修正済み計算機ＩＤなどの固有のターゲット・コンピュータ属性７０５で鍵がかけられている。暗号化操作６９９の出力は、製品キー（ソース・コンピュータ６５１のキー・ファイル６５３の一時製品キーと同じ）、顧客番号（ソース・コンピュータ６５１のキー・ファイル６５３の顧客番号と同じ）、クリア計算機ＩＤ（ターゲット・コンピュータ７０７用の計算機ＩＤであって、ソース・コンピュータ６５１の計算機ＩＤではない）、試用期間データ（ソース・コンピュータ６５１のキー・ファイル６５３の試用期間データと同じ）、およびソース・コンピュータ６５１の計算機ＩＤのＩＤを含む暗号化キー・ファイル７０９を生成する。暗号化操作７０３の出力は計算機ＩＤファイル７１１を定義するもので、このファイルは、ターゲット・コンピュータ７０７の計算機ＩＤ（ソース・コンピュータ６５１の計算機ＩＤではない）と試用期間データ（ソース・コンピュータ６５１の計算機ＩＤファイル６５５の試用期間データと同じ）とを含む。

【００６６】図３４および図３５は、図３２および図３３に示したインポート操作とエクスポート操作の代替図で、本発明の重要な特徴の一部を強調するものである。図示の通り、ソース・コンピュータ８０１は、ソース・コンピュータ８０１に固有のシステム属性キーで暗号化された計算機ＩＤファイル８０３を含む。この計算機ＩＤファイルは、計算機ＩＤファイル番号ならびに各保護ソフトウェア製品ごとに許されるエクスポートの回数を示すカウントと、使用されたエクスポートの総数を示すカウントとを含む。たとえば、最初のエクスポート操作で”１：１０”というカウントが伝達された場合、許可された１０回のエクスポート操作のうちの１回が行われたことを意味する。次のエクスポート操作では、カウンタは”２：１０”に増加し、許可された１０回のエクスポート操作のうち２回が行われたことを意味する。特定のエクスポート操作の受取り側であることを示すために、エクスポート操作の結果を受け取る各ターゲット・コンピュータには、この特定のカウンタ値でタグが付けられる。たとえば、１つのソース・コンピュータ・システムが”１：１０”というカウンタ値を有する場合、このシステムが許可された１０回のエクスポート操作のうちの最初のエクスポート操作の受取り側であることを意味する。さらに別のターゲット・コンピュータが”７：１０”というカウンタ値を有する場合は、この特定のターゲット・コンピュータが許可された１０回のエクスポート操作のうちの７回目のエクスポート操作を受け取ったことを意味する。このようにして、ターゲット・コンピュータは使用したエクスポート操作の総数のカウントを保管するのに対し、それぞれのソース・コンピュータは、許可された複数のエクスポート操作のうちの特定の操作による計算機ＩＤファイルとキー・ファイルの受取り側を識別するための異なるカウンタ値を有する。

【００６７】ソース・コンピュータ８０１では、ソース・コンピュータ８０１に固有のシステム属性をキーとして使用する暗号化アルゴリズムによって計算機ＩＤファイル８０３とキー・ファイル８０５が暗号化されるが、計算機ＩＤファイル８０３とキー・ファイル８０５がエクスポート・キー・ディスケット８０７などのメモリ媒体に転送されると、ディスケットの製造番号などの固有のディスケット属性を暗号化キーとして使用する従来の暗号化操作で計算機ＩＤファイル８０９とキー・ファイル８１１が暗号化されることに留意されたい。これにより、計算機ＩＤファイル８０９またはキー・ファイル８１１あるいはその両方の内容が別のディスケットまたは他のメモリ媒体にコピーされ、ソフトウェア製品への無許可アクセスを獲得するのに利用される可能性が最小限に抑えられる。その理由は、計算機ＩＤファイル８０９とキー・ファイル８１１の内容を効果的にターゲット・コンピュータに転送するために、ターゲット・コンピュータはエクスポート・キー・ディスケット８０７から固有のディスケット属性を読み取って使用できなければならないためである。計算機ＩＤファイル８０９とキー・ファイル８１１がコピーされているディスケットでこれらのファイルがターゲット・コンピュータに提供された場合のみ、効果的な転送を行うことができる。暗号解読操作を正常に実施するにはターゲット・コンピュータはエクスポート・キー・ディスケット８０７の固有の属性（ディスケット製造番号など）を必要とするため、潜在

的ターゲット・コンピュータに対してエクスポート・キー・ディスケット８０７以外のディスケットで計算機ＩＤファイル８０９とキー・ファイル８１１を提供すると、無意味な情報が転送されてしまう。

【００６８】図３５に示すように、エクスポート・キー・ディスケット８０７はターゲット・コンピュータ８１３に提供される。当然のことながら、計算機ＩＤファイル８０９とキー・ファイル８１１は暗号化形式になっている。エクスポート・キー・ディスケット８０７からターゲット・コンピュータ８１３に転送する場合、計算機ＩＤファイル８０９の内容は、ターゲット・コンピュータ８１３の計算機ＩＤと、使用したインポート操作のカウントで更新される。ターゲット・コンピュータ８１３への転送を実施する場合、ターゲット・コンピュータ８１３用の計算機ＩＤなどの複数の項目と、顧客情報、ならびにソース・コンピュータ８０１の計算機ＩＤ番号のリストを含む計算機ＩＤファイル８１５が作成される。計算機ＩＤファイル８１５とキー・ファイル８１７はどちらも、ターゲット・コンピュータ８１３の固有の属性をキーとして使用する従来の暗号化操作を使用して暗号化される。これにより、計算機ＩＤファイル８１５およびキー・ファイル８１７が特定のターゲット・コンピュータ８１３に結びつけられる。

【００６９】エクスポート／インポート・カウンタを使用して、許可されたエクスポート／インポート操作の総数と使用したエクスポート／インポート操作の総数を追跡することで、本発明は、試用期間中にソフトウェア製品の配布を追跡するのに使用可能な監査証跡（audit trail）を作成する。各ソース・コンピュータは、実行されたエクスポート操作の総数の記録を保有する。また、各ソース・コンピュータは、どの特定のエクスポート／インポート操作が１つまたは複数の保護ソフトウェア製品をターゲット・コンピュータに転送するのに使用されたかについての記録も保有する。この転送を実施するのに使用するメモリ媒体（１枚のディスケットまたは１群のディスケットなど）は、すべてのエクスポート／インポート操作に使用されたソース・コンピュータとターゲット・コンピュータの両方の計算機ＩＤ番号の永続的記録を保有する。

【００７０】エクスポート操作とインポート操作を実施するための手順により、保護ソフトウェア製品が不必要な危険に曝されることがなくなる。計算機ＩＤファイルとキー・ファイルがソース・コンピュータからターゲット・コンピュータに渡されると、エクスポート・ディスケットをコピーしたり、不当にキーを配布するための手段としてその内容を掲示板に掲載する行為を防止または禁止するエクスポート・ディスケットの固有の属性によって、これらのファイルが暗号化される。インポート操作時は、ソース・コンピュータの安全保護と一致するようにソフトウェア製品が維持されることを保証するため、計算機ＩＤファイルとキー・ファイルがターゲット・コンピュータに固有のシステム属性で暗号化される。ただし、ソフトウェア製品そのものはターゲット・コンピュータに固有の属性で暗号化される。その結果、キーの不当コピーや掲載が防止される。

【００７１】エクスポート／インポート機能の第二の実施例は、図３６および図３７にブロック図形式で示す。大まかに概説すると、まず、メモリ媒体１６７７を使用してターゲット・コンピュータ１７０７とやりとりし、ターゲット・コンピュータ１７０７に固有で、好ましくはターゲット・コンピュータ１７０７の１つまたは複数の固有のシステム属性から導出される転送キーをターゲット・コンピュータ１７０７から獲得する。この転送キーは、ターゲット・コンピュータ１７０７用の計算機ＩＤの修正版でもよい。次に、メモリ媒体１６７７を使用してエクスポート動作モードでソース・コンピュータ１６５１とやりとりする。そのモードではキー・ファイル１６５３と計算機ＩＤファイル１６５５がまず暗号解読され、その後、転送キーを使用して暗号化される。

【００７２】図３６は、本発明の好ましい実施例によるエクスポート操作を示すブロック図である。図示の通り、ソース・コンピュータ１６５１は、キー・ファイル１６５３と計算機ＩＤファイル１６５５とを含む。キー・ファイル１６５３は、製品キーと、顧客キーと、ソース・コンピュータ１６５１用の計算機ＩＤのクリア・テキストと、試用期間データ（試用期間を定義するクロックまたはカウンタあるいはその両方など）と、特定の保護ソフトウェア製品について許可されたエクスポート操作の最大数を定義し、実施されたエクスポート操作の総数を追跡するという二重機能を実行するエクスポート・カウンタとを含む。計算機ＩＤファイルは、計算機ＩＤ番号と試用期間データ（試用期間を定義するクロックまたはカウンタあるいはその両方など）とを含む。キー・ファイル１６５３と計算機ＩＤファイル１６５５はどちらも従来の暗号化操作（ＤＥＳアルゴリズムなど）によって暗号化されるが、この操作はソース・コンピュータ１６５１の固有のシステム属性から導出されるキーで鍵がかけられている。エクスポート操作の開始時に、キー・ファイル１６５３と計算機ＩＤファイル１６５５が暗号解読される。キー・ファイル１６５３は、キー１６５９で鍵がかけられた暗号解読操作１６５７に入力として供給される。同様に、計算機ＩＤファイル１６５５は、キー１６６１で鍵がかけられた暗号解読操作１６６３に入力として供給される。暗号解読操作１６５７および１６６３は、キー・ファイル１６５３と計算機ＩＤファイル１６５５のクリア・テキスト・バージョンを生成する。クリア・テキストが得られると、キー・ファイル１６５３内に収容されているエクスポート・カウンタがブロック１６６１により修正される。たとえば、この操作が、許される１０回の操作のうちの７回目のエクスポー

ト操作であれば、カウンタは”７：１０”と表示するはずである。キー・ファイル１６５３のクリア・テキスト・バージョンは暗号化操作１６６９に入力として供給される。この暗号化操作１６６９は、従来のいずれの暗号化操作（ＤＥＳアルゴリズムなど）でもよく、前に得られた転送キー１６６５で鍵がかけられる。計算機ＩＤファイル１６５５のクリア・テキストについても同じ操作が行われる。すなわち、転送キー１６７１が暗号化操作１６７５のキーとして使用される。この暗号化操作は、ＤＥＳ操作などの従来の暗号化操作で構成することができる。最後に、暗号化操作１６６９および１６７５の出力がコピー操作１６７９および１６８１に入力として供給され、暗号化キー・ファイル１６５３と計算機ＩＤファイル１６５５がメモリ媒体１６７７にコピーされる。

【００７３】図３７は、インポート操作を示すブロック図である。メモリ媒体１６７７（図３６）はソース・コンピュータ１６５１（図３６）から物理的に取り外され、コンピュータ１７０７（図３７）に物理的に運搬される。あるいは、分散データ処理システムではこの転送は、メモリ媒体１６７７の物理的な取外しを伴わずに行われる場合もある。ここで図３７に関して説明すると、どの特定のターゲット・コンピュータがキー・ファイルと計算機ＩＤファイルを受け取ったかを記録するために、ブロック１６８３により、ターゲット・コンピュータの計算機ＩＤがメモリ媒体１６７７にコピーされる。次に、ブロック１６８５および１６９３により、暗号化キー・ファイル１６５３と計算機ＩＤファイル１６５５がメモリ媒体からターゲット・コンピュータ１７０７にコピーされる。暗号化キー・ファイル１６５３は、キー１６８７で鍵がかけられた暗号解読操作１６８９に入力として供給される。暗号解読操作１６８９は、ブロック１６６９の暗号化操作を取り消すもので、キー・ファイル１６５３のクリア・テキスト・バージョンを出力として提供する。同様に、計算機ＩＤファイル１６５５は、キー１６９５で鍵がかけられた暗号解読操作１６９７に入力として供給される。暗号解読操作１６９７は、暗号化操作１６７５の暗号化を取り消すもので、計算機ＩＤファイル１６５５のクリア・テキストを出力として提供する。ブロック１６９１により、ソース・コンピュータ１６５１の計算機ＩＤが取り出され、キー・ファイル１６５３のクリア・テキストとしてメモリ内に記録される。次に、キー・ファイル１６５３のクリア・テキストが暗号化操作１６９９に入力として供給される。暗号化操作１６９９は、ＤＥＳ操作などの従来の暗号化操作であり、ターゲット・コンピュータ１７０７用の計算機ＩＤまたは修正済み計算機ＩＤなどのターゲット・コンピュータ固有の属性で鍵がかけられている。計算機ＩＤファイル１６５５のクリア・テキストは、暗号化操作１７０３に入力として供給される。この暗号化操作１７０３は、ＤＥＳ暗号化操作などの従来の暗号化操作であり、ターゲット・コンピュータ１７０７の計算機ＩＤまたは修正済み計算機ＩＤなどの固有のターゲット・コンピュータ属性１７０５で鍵がかけられている。暗号化操作１６９９の出力は、製品キー（ソース・コンピュータ１６５１のキー・ファイル１６５３の一時製品キーと同じ）、顧客番号（ソース・コンピュータ１６５１のキー・ファイル１６５３の顧客番号と同じ）、クリア計算機ＩＤ（ターゲット・コンピュータ１７０７用の計算機ＩＤであって、ソース・コンピュータ１６５１の計算機ＩＤではない）、試用期間データ（ソース・コンピュータ１６５１のキー・ファイル１６５３の試用期間データと同じ）、およびソース・コンピュータ１６５１の計算機ＩＤのＩＤを含む暗号化キー・ファイル１７０９を生成する。暗号化操作１７０３の出力は計算機ＩＤファイル１７１１を定義するもので、このファイルは、ターゲット・コンピュータ１７０７の計算機ＩＤ（ソース・コンピュータ１６５１の計算機ＩＤではない）と試用期間データ（ソース・コンピュータ１６５１の計算機ＩＤファイル１６５５の試用期間データと同じ）とを含む。

【００７４】まとめとして、本発明の構成に関して以下の事項を開示する。

【００７５】（１）供給側であるソースからユーザにソフトウェア・オブジェクトを配布する方法において、永続暗号化キーを使用する暗号化操作で前記ソフトウェア・オブジェクトを暗号化するステップと、前記ソースから前記ユーザに前記暗号化ソフトウェア・オブジェクトを送るステップと、特定のシステム構成を有するユーザ制御のデータ処理システムに前記暗号化ソフトウェア・オブジェクトをロードするステップと、少なくとも一部が前記システム構成に基づく計算機ＩＤを導出するステップと、少なくとも一部が前記計算機ＩＤと前記永続暗号化キーとに基づく一時キーを導出するステップと、所定の期間、前記ユーザが前記一時キーを使用して前記永続暗号化キーを生成できるように、前記一時キーを受け取って、前記永続暗号化キーを生成するための永続キー生成機能を動作させ、前記ソフトウェア・オブジェクトへのアクセスを可能にするステップとを含む方法。

（２）前記暗号化ソフトウェア・オブジェクトが、コンピュータがアクセス可能なメモリ媒体上に記録されて、前記ソースから前記ユーザに送られる、上記（１）に記載のソフトウェア・オブジェクトを配布する方法。

（３）前記永続キー生成機能が、前記コンピュータがアクセス可能なメモリ媒体上に保持され、前記暗号化ソフトウェア・オブジェクトとともに前記ソースから前記ユーザに送られる、上記（２）に記載のソフトウェア・オブジェクトを配布する方法。

（４）前記永続キー生成機能をその構成要素として含む、ファイル管理プログラムを、　前記暗号化ソフトウェア・オブジェクトとともに前記ソースから前記ユーザに送るステップをさらに含む、上記（１）に記載のソフ

トウェア・オブジェクトを配布する方法。
（５）少なくとも前記一時キーを記録するために前記ユーザ制御のデータ処理システム内にキー・ファイルを作成するステップを含む、上記（１）に記載のソフトウェア・オブジェクトを配布する方法。
（６）少なくとも１つの固有のシステム属性を暗号化キーとして使用して、前記キー・ファイルを暗号化するステップを含む、上記（５）に記載のソフトウェア・オブジェクトを配布する方法。
（７）作成者からユーザにソフトウェア・オブジェクトを配布する方法において、永続キーを使用して前記ソフトウェア・オブジェクトを暗号化するステップと、前記ソフトウェア・オブジェクトをコンピュータがアクセス可能なメモリ媒体にファイル管理プログラムとともに記録するステップと、前記作成者から前記ユーザに前記コンピュータがアクセス可能なメモリを発送するステップと、前記ファイル管理プログラムをユーザ制御のデータ処理システムにロードし、それを前記ユーザ制御のデータ処理システム用のオペレーティング・システムに関連付けるステップと、前記ファイル管理プログラムを使用して、前記ユーザ制御のデータ処理システムの少なくとも１つの属性に基づく計算機ＩＤを導出するステップと、前記ユーザ制御のデータ処理システムで前記コンピュータがアクセス可能なメモリを読み取るステップと、少なくとも一部が前記計算機ＩＤに基づく一時キーを導出するステップと、前記ユーザ制御のデータ処理システムで前記ファイル管理プログラムを実行することにより、前記一時キーによって定義される期間の間、前記ソフトウェア・オブジェクトへのアクセスを制限するステップと、前記ユーザ制御のデータ処理システムにおいて永続キー生成機能を実行することにより、少なくとも前記一時キーを受け取ったことに対する応答として前記永続キーを提供するステップとを含む方法。
（８）前記ファイル管理プログラムが、前記ユーザ制御のデータ処理システムによって実行されるときに、複数の動作モードで動作可能であり、（ａ）前記一時キーを使用することで前記ソフトウェア・オブジェクトが一時的に使用可能になる一時試用動作モードと、（ｂ）前記ソフトウェア・オブジェクトを永続的に使用可能にして、前記ユーザによる前記ソフトウェア・オブジェクトの無制限使用を可能にする永続使用動作モードとを含むことを特徴とする、上記（７）に記載のソフトウェア・オブジェクトを配布する方法。
【００７６】
【発明の効果】本発明のソフトウェア配布手法により、不正使用の問題を回避しつつ、ユーザに一次的な一定の試用期間を許容する機構が提供される。しかも、当該試用期間後もソフトウェア製品の使用を望むユーザについては、別途永続キーを付与することによりその目的が達成される。

【図面の簡単な説明】
【図１】ソフトウェア製品の試用期間使用を可能にする好ましい技法を実施する際に使用可能なスタンドアロン型データ処理システム、電話、およびコンピュータがアクセス可能な様々なメモリ媒体を示す絵画表現である。
【図２】ソフトウェア製品の試用期間使用を可能にする本発明の技法を使用可能な分散データ処理システムを示す絵画表現である。
【図３】本発明により計算機ＩＤを生成するために使用可能なデータ処理システムの属性を示すブロック図である。
【図４】ソフトウェア・オブジェクトを暗号化するためのルーチンを示すブロック図である。
【図５】本発明の教示によりソース（ソフトウェア・ベンダ）とユーザ（顧客）との間で行われる情報交換を示す絵画表現である。
【図６】本発明によりユーザ・インタフェース・シェルを構築する際に使用される大まかなステップを示す流れ図である。
【図７】本発明によるベンダと顧客との対話を示す流れ図である。
【図８】本発明による試用期間操作を容易にするためのユーザ・インタフェース画面を示す図である。
【図９】本発明による試用期間操作を容易にするためのユーザ・インタフェース画面を示す図である。
【図１０】本発明による試用期間操作を容易にするためのユーザ・インタフェース画面を示す図である。
【図１１】本発明による試用期間操作を容易にするためのユーザ・インタフェース画面を示す図である。
【図１２】一時アクセス・キーを開始するために使用されるユーザ・インタフェースを示す図である。
【図１３】計算機ＩＤを生成する好ましい技法を示すブロック図である。
【図１４】本発明により計算機ＩＤを暗号化するために使用される暗号化操作を示すブロック図である。
【図１５】本発明により製品キーを生成する好ましい技法を示すブロック図である。
【図１６】１つまたは複数のソフトウェア・オブジェクトの暗号解読に使用可能な実キーを生成するために一時製品キーを使用する好ましい技法を示すブロック図である。
【図１７】図１６のブロック図により導出された実キーの妥当性を検査する好ましい技法を示す図である。
【図１８】図１６のブロック図により導出された実キーの妥当性を検査する好ましい技法を示す図である。
【図１９】一時製品キーを含む情報が入っているキー・ファイルを暗号化するための好ましいルーチンを示すブロック図である。
【図２０】本発明により暗号化ファイル内の暗号化ヘッダを処理する好ましい技法を示すブロック図である。

【図２１】暗号化ソフトウェア・オブジェクトの暗号解読に使用可能な実キーを導出するためにユーザ制御のデータ処理システム内の複数の入力を使用する技法を示すブロック図である。

【図２２】図２１により導出された実キーを使用する暗号解読操作を示す図である。

【図２３】実キーの妥当性を判定するために使用される比較操作を示すブロック図である。

【図２４】妥当性が検査された実キーを使用する暗号解読操作を示す図である。

【図２５】本発明による暗号化ヘッダの使い方を示す図である。

【図２６】本発明による暗号化ヘッダの使い方を示す図である。

【図２７】本発明による暗号化ヘッダの使い方を示す図である。

【図２８】本発明による暗号化ヘッダの使い方を示す図である。

【図２９】本発明による暗号化ヘッダの使い方を示す図である。

【図３０】暗号化ソフトウェア・オブジェクトに関して試用期間使用を提供する好ましい技法を示す流れ図である。

【図３１】暗号化ソフトウェア・オブジェクトに関して試用期間使用を提供する好ましい技法を示す流れ図である。

【図３２】分散データ処理システム内で試用期間使用操作を実行するために使用可能なエクスポート操作を示す図である。

【図３３】分散データ処理システム内で試用期間使用操作を実行するために使用可能なインポート操作を示す図である。

【図３４】図３２に示すエクスポート操作の代替図である。

【図３５】図３３に示すインポート操作の代替図である。

【図３６】エクスポート操作を実行するための代替技法を示すブロック図である。

【図３７】インポート操作を実行するための代替技法を示すブロック図である。

【符号の説明】

２０９　ソース、ベンダ

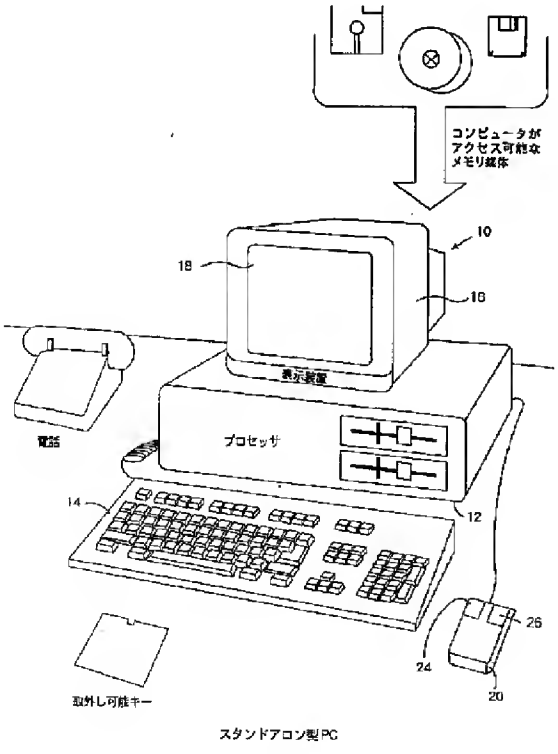
２１１　ユーザ、顧客

２１３　メモリ媒体

２１５　ユーザ固有情報、計算機ＩＤ

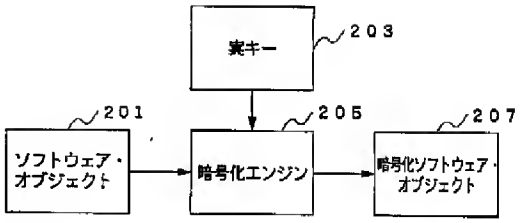
２１７　製品キー、顧客番号

【図１】

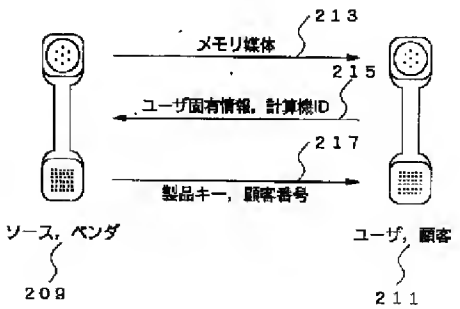


スタンドアロン型PC

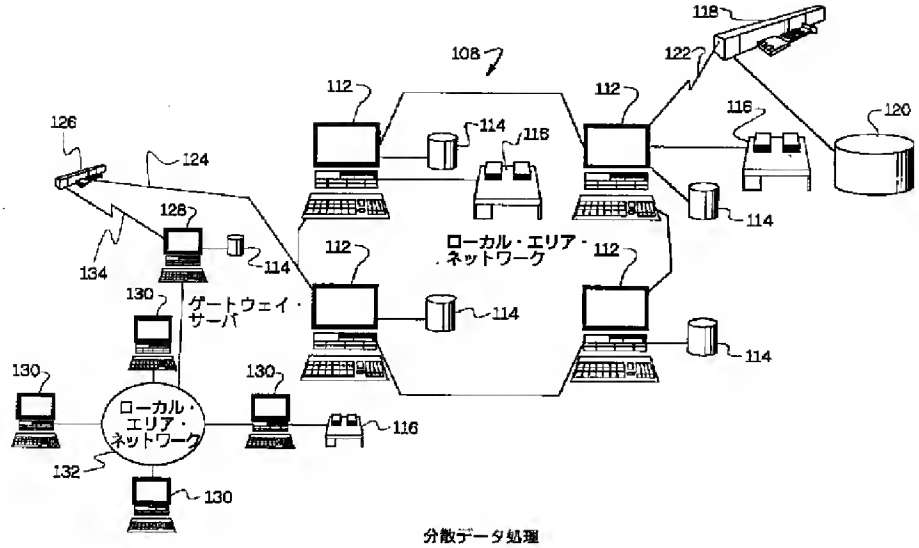
【図４】



【図５】

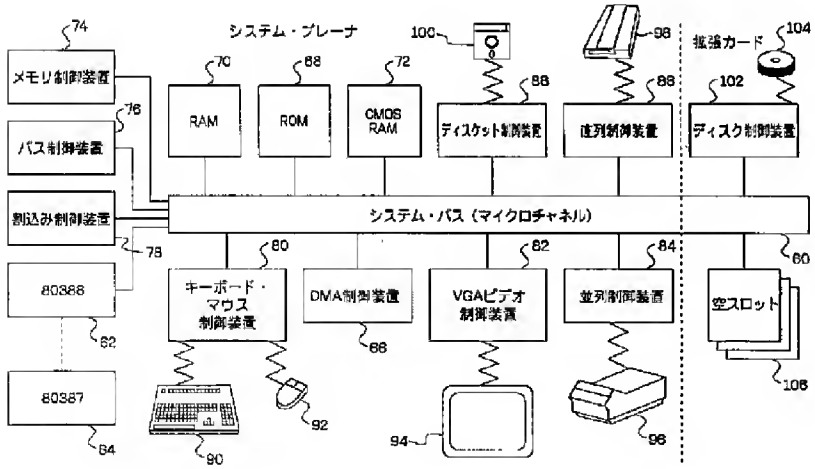


【図２】

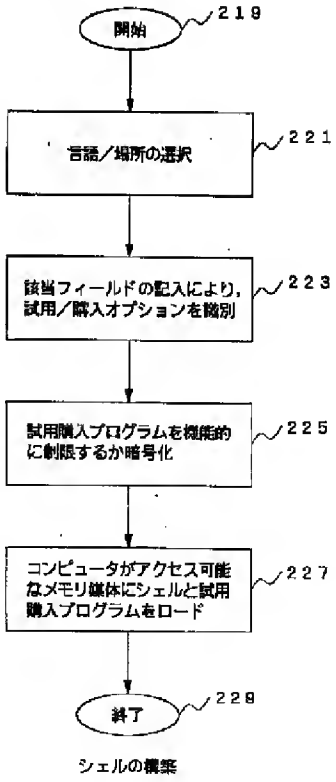


分散データ処理

【図３】

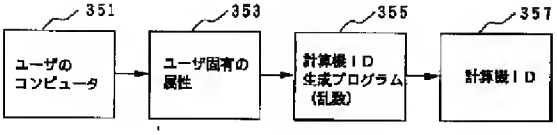


【図６】

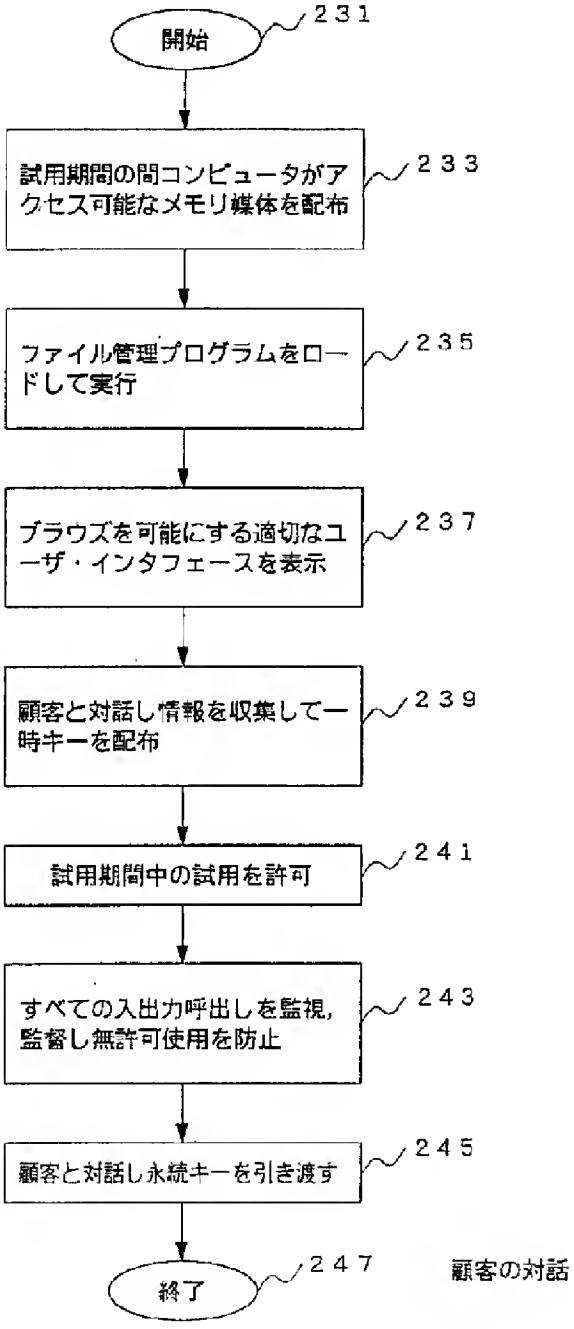


シェルの構築

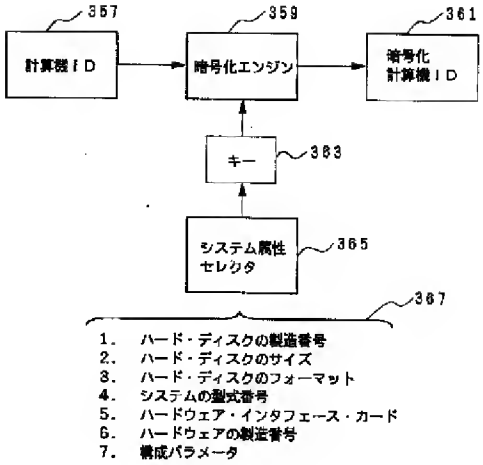
【図１３】



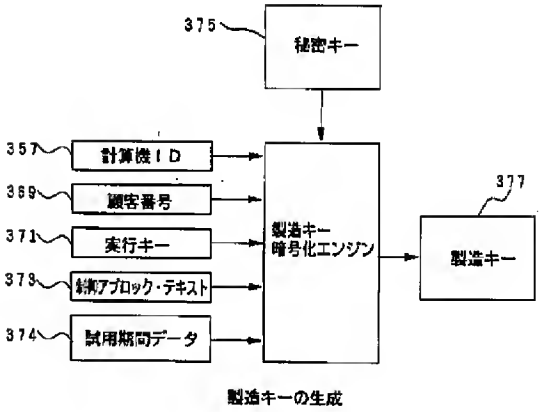
【図７】



【図１４】

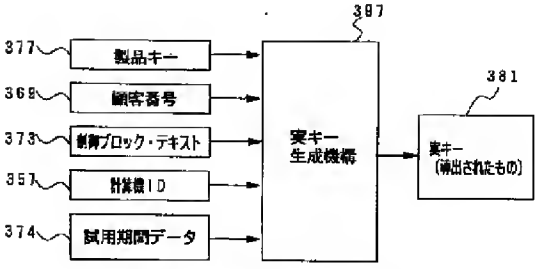


【図１５】



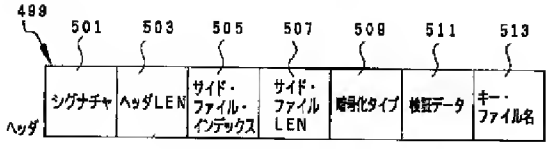
製造キーの生成

【図１６】

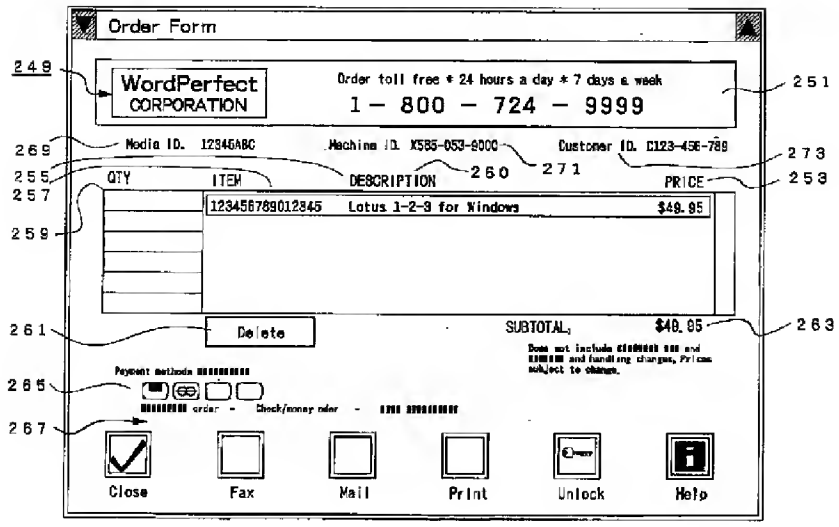


製品キーの妥当性検査

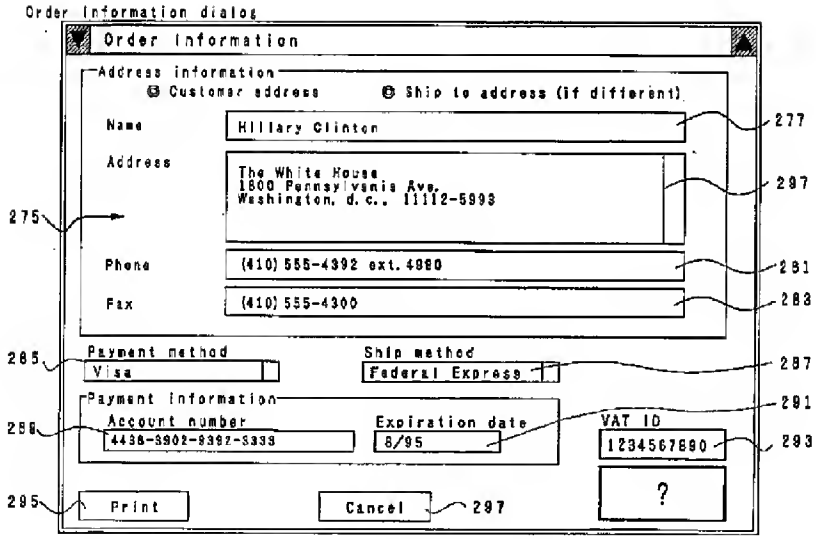
【図２７】



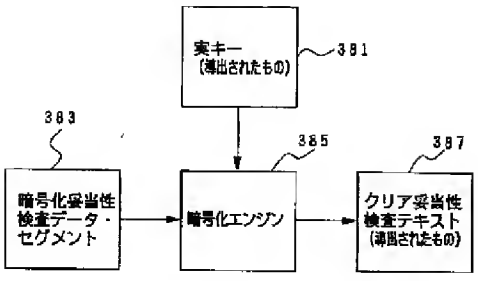
【図８】


Order Form
249
WordPerfect
CORPORATION
Order toll free * 24 hours a day * 7 days a week
1 - 800 - 724 - 9999
251
269
Media ID. 12345ABC
Machine ID. X585-053-8000
Customer ID. C123-456-789
273
255
DESCRIPTION
260
271
PRICE
253
257
QTY
ITEM
259
1234567890123845 Lotus 1-2-3 for Windows $49.95
261
Delete
SUBTOTAL: $49.95
263
265
267
Close
Fax
Mail
Print
Unlock
Help

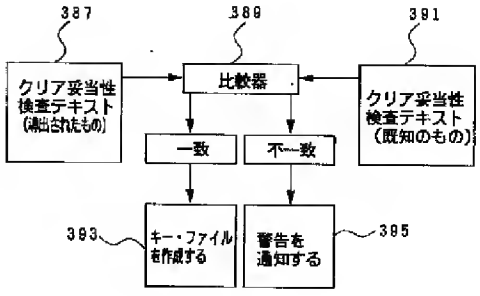
【図９】


Order Information dialog
Order Information
Address information
Customer address
Ship to address (if different)
Name
Hillary Clinton
277
Address
The White House
1600 Pennsylvania Ave.
Washington, d.c., 11112-5993
279
275
Phone
(410) 555-4392 ext. 4980
281
Fax
(410) 555-4300
283
Payment method
Visa
Ship method
Federal Express
285
287
Payment information
Account number
4438-3902-9392-3333
Expiration date
8/95
291
289
VAT ID
1234567890
293
?
295
Print
Cancel
297

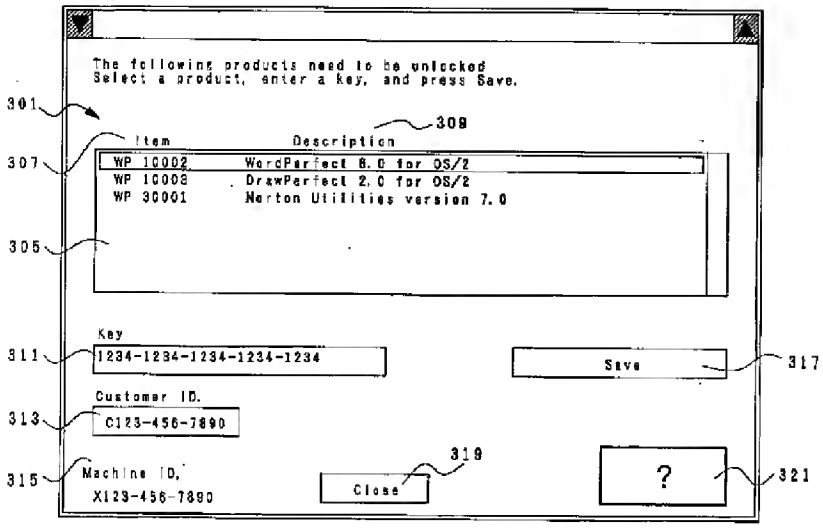
【図１７】


実キー
(導出されたもの)
381
383
385
387
暗号化妥当性
検査データ・
セグメント
暗号化エンジン
クリア妥当性
検査テキスト
(導出されたもの)

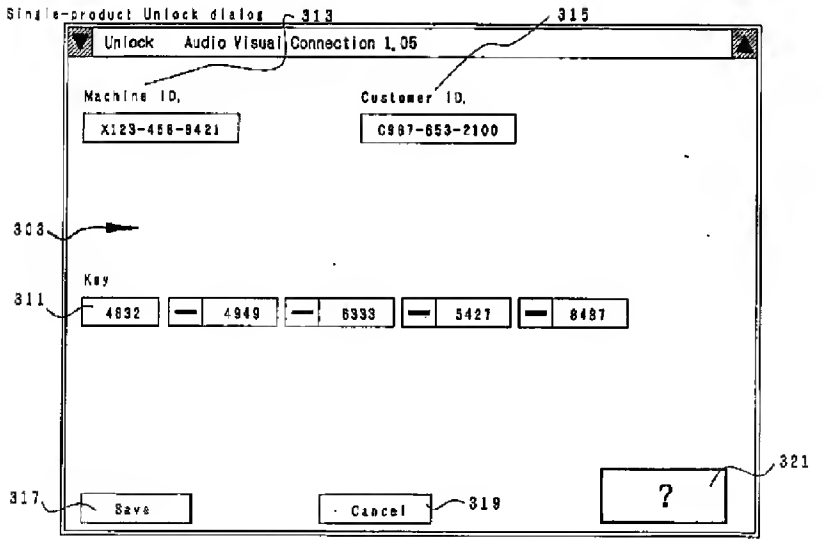
【図１８】


387
389
391
クリア妥当性
検査テキスト
(導出されたもの)
比較器
クリア妥当性
検査テキスト
(既知のもの)
一致
不一致
393
キー・ファイル
を作成する
警告を
通知する
395

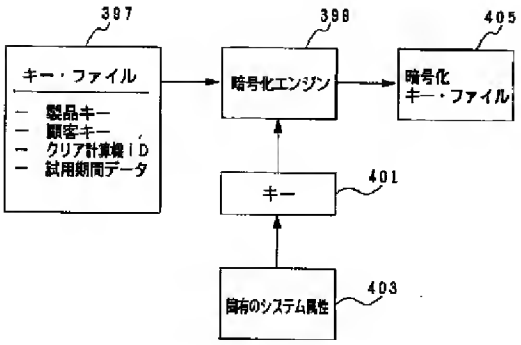
【図１０】



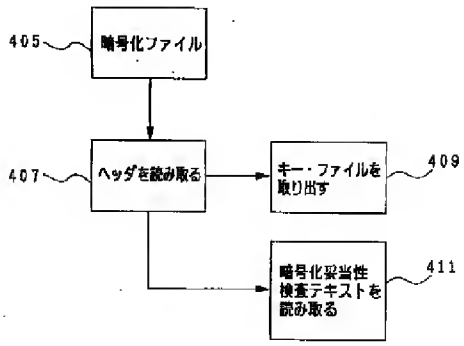
【図１１】



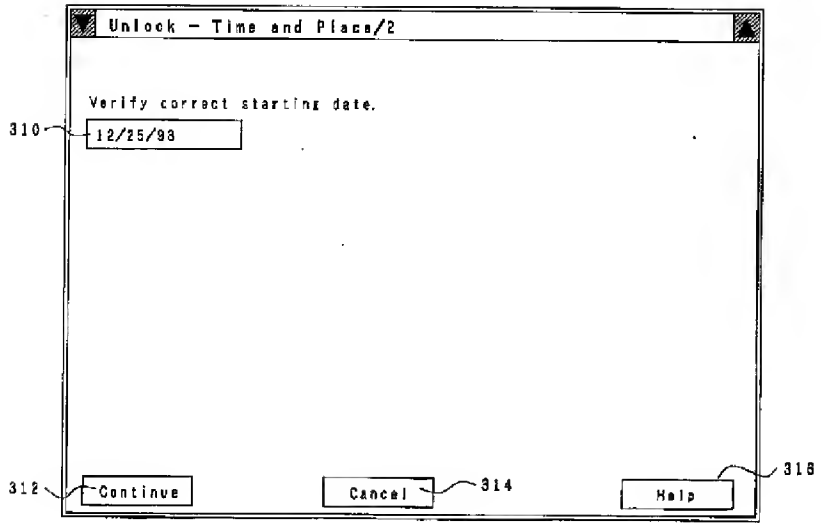
【図１９】



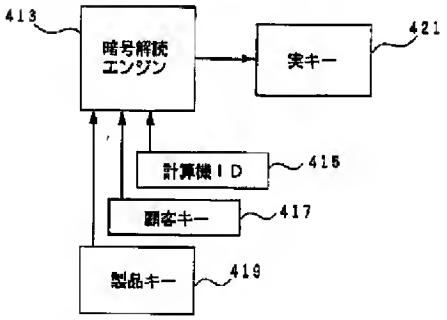
【図２０】



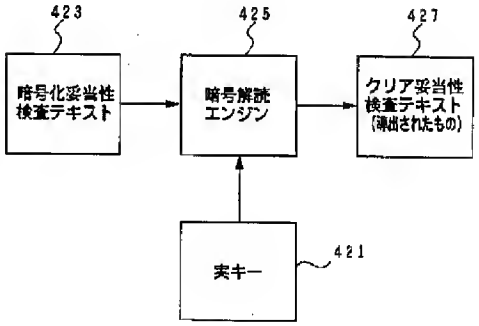
【図１２】



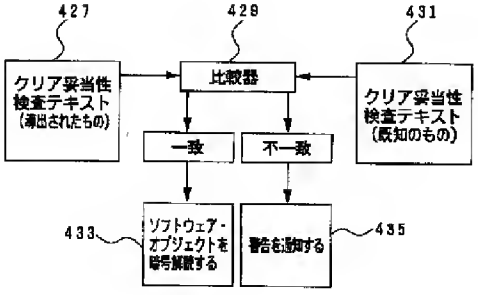
【図２１】



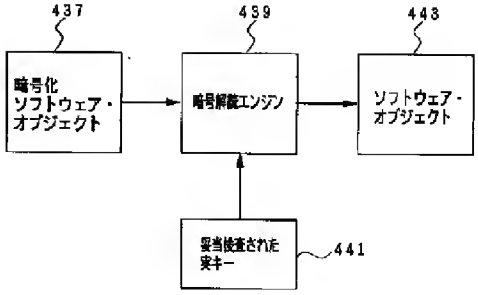
【図２２】



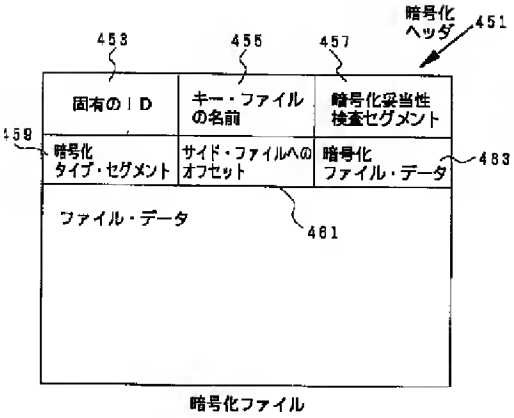
【図２３】



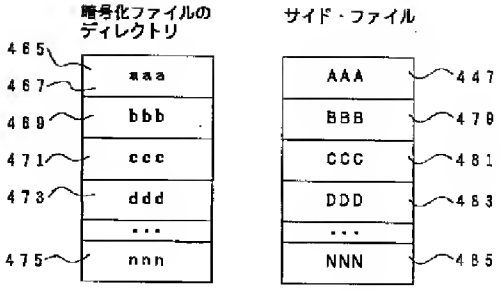
【図２４】



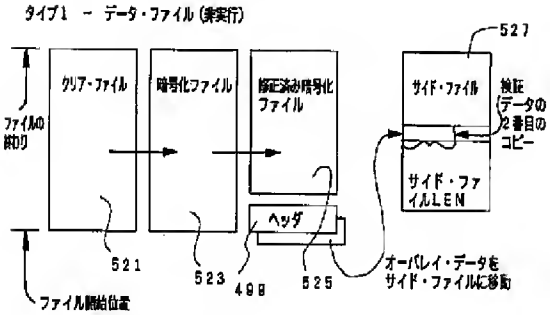
【図２５】



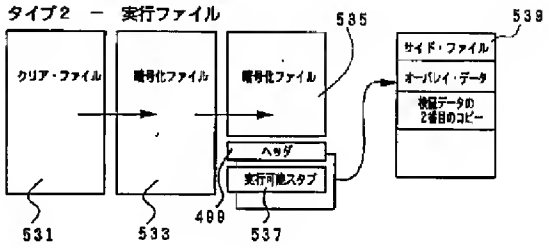
【図２６】



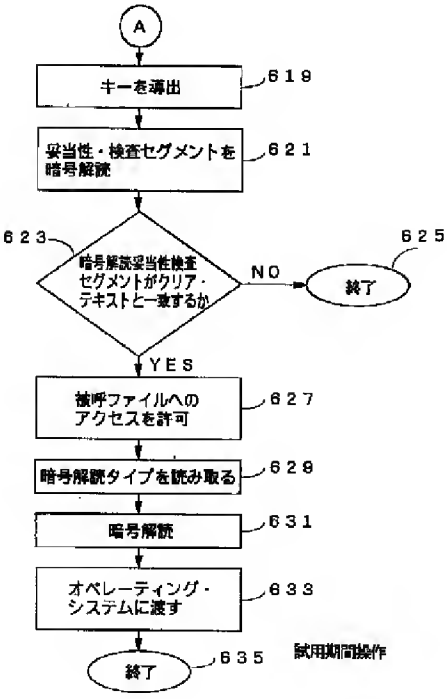
【図２８】



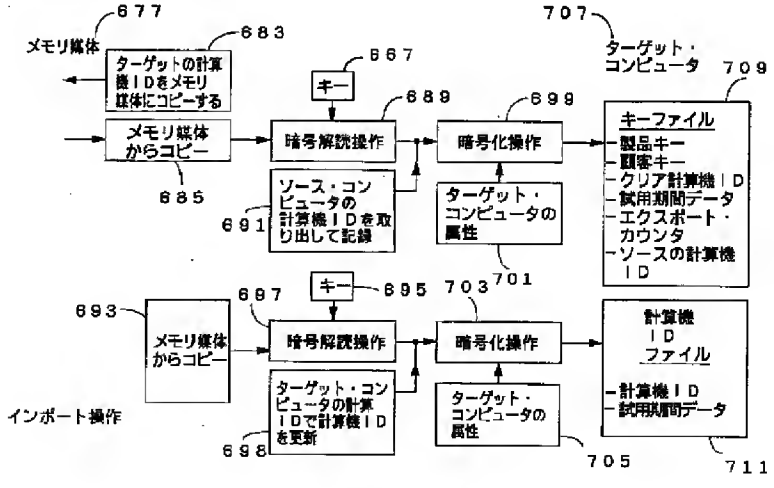
【図２９】



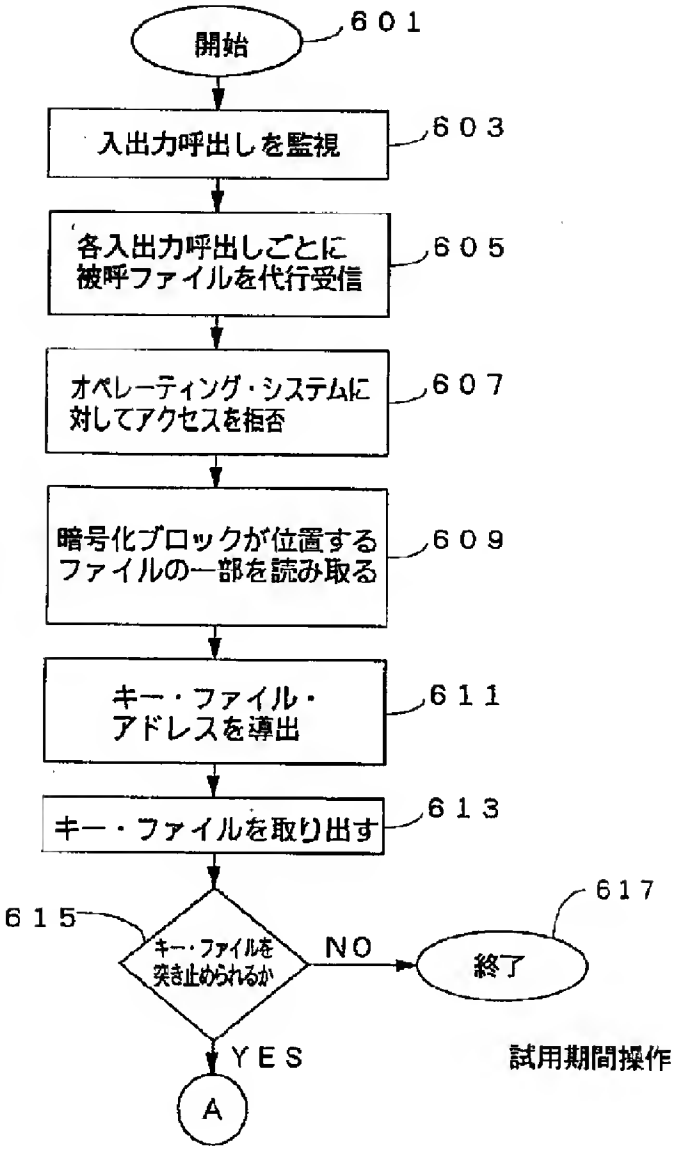
【図３１】



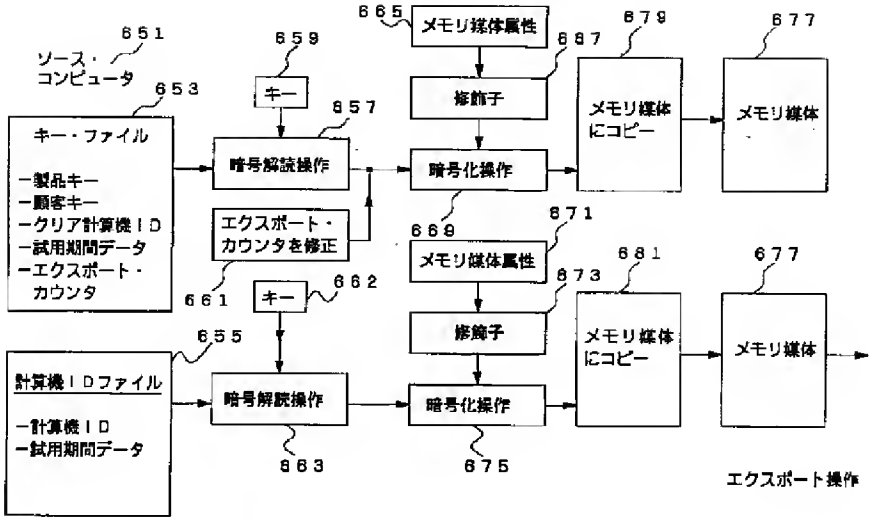
【図３３】



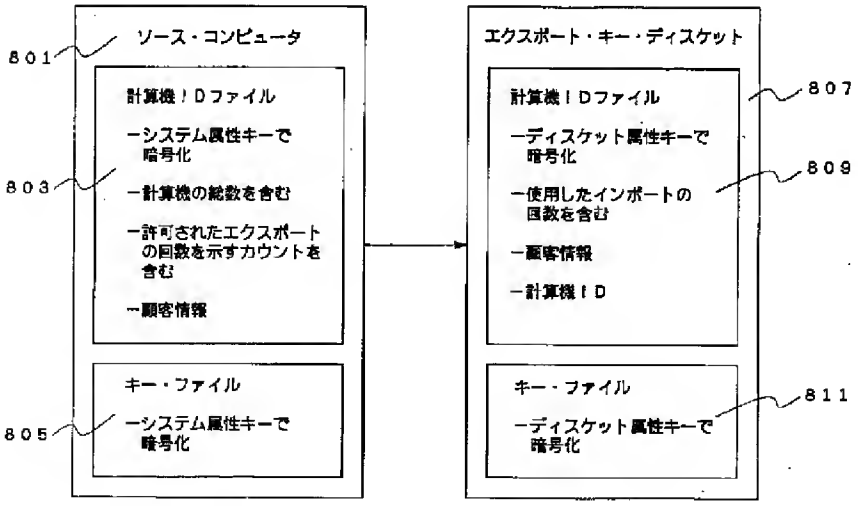
【図３０】


開始
601
入出力呼出しを監視
603
各入出力呼出しごとに
被呼ファイルを代行受信
605
オペレーティング・システムに
対してアクセスを拒否
607
暗号化ブロックが位置する
ファイルの一部を読み取る
609
キー・ファイル・
アドレスを導出
611
キー・ファイルを取り出す
613
615
キー・ファイルを
突き止められるか
NO
617
終了
YES
A
試用期間操作

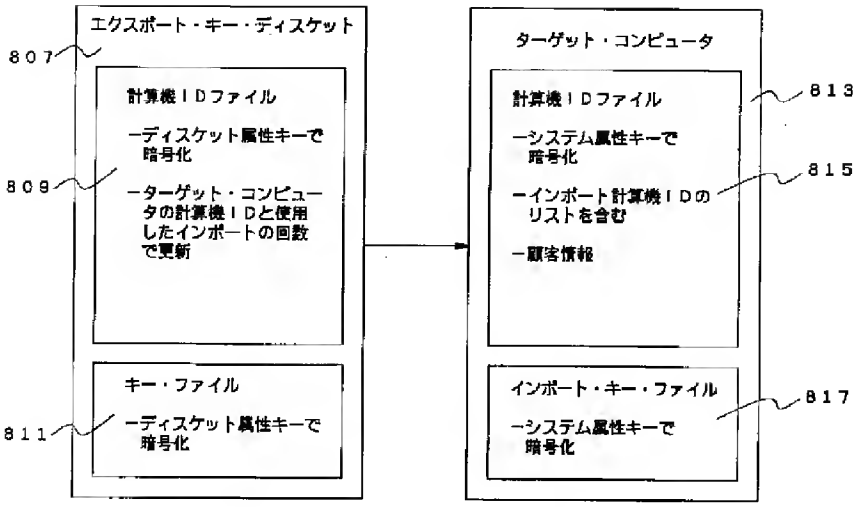
【図３２】


651
ソース・
コンピュータ
653
キー・ファイル
－製品キー
－顧客キー
－クリア計算機ＩＤ
－試用期間データ
－エクスポート・
カウンタ
659
キー
657
暗号解読操作
エクスポート・
カウンタを修正
661
キー
662
655
計算機ＩＤファイル
－計算機ＩＤ
－試用期間データ
暗号解読操作
663
665
メモリ媒体属性
667
修飾子
暗号化操作
669
671
メモリ媒体属性
673
修飾子
暗号化操作
675
679
メモリ媒体
にコピー
681
メモリ媒体
にコピー
677
メモリ媒体
677
メモリ媒体
エクスポート操作

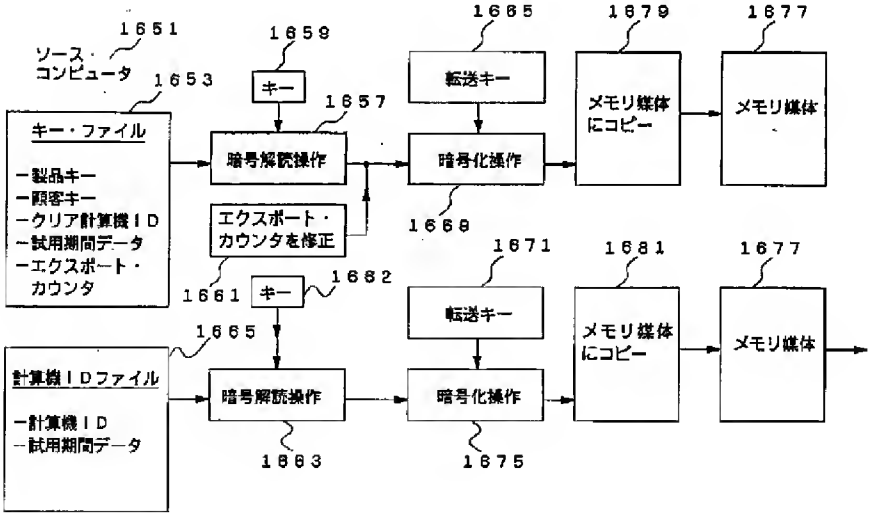
【図３４】


801
ソース・コンピュータ
803
計算機ＩＤファイル
－システム属性キーで
暗号化
－計算機の総数を含む
－許可されたエクスポート
の回数を示すカウントを
含む
－顧客情報
805
キー・ファイル
－システム属性キーで
暗号化
エクスポート・キー・ディスケット
807
計算機ＩＤファイル
－ディスケット属性キーで
暗号化
809
－使用したインポートの
回数を含む
－顧客情報
－計算機ＩＤ
811
キー・ファイル
－ディスケット属性キーで
暗号化

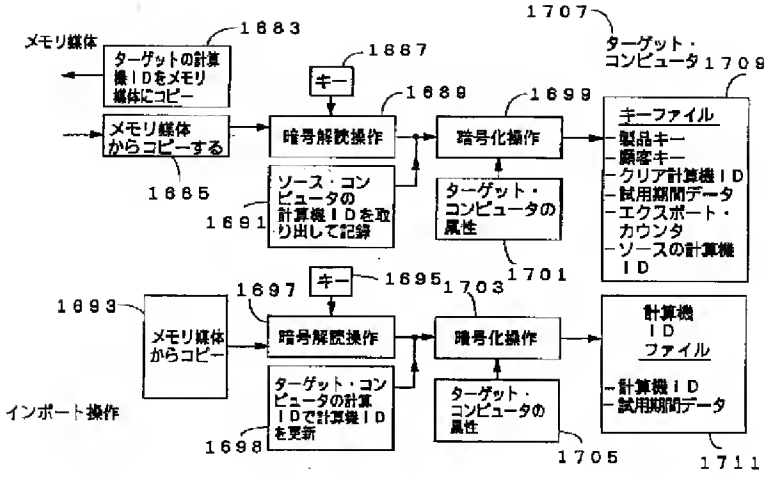
【図３５】


エクスポート・キー・ディスケット
807
計算機ＩＤファイル
－ディスケット属性キーで暗号化
809
－ターゲット・コンピュータの計算機ＩＤと使用したインポートの回数で更新
キー・ファイル
－ディスケット属性キーで暗号化
811
ターゲット・コンピュータ
計算機ＩＤファイル
－システム属性キーで暗号化
－インポート計算機ＩＤのリストを含む
－顧客情報
813
815
インポート・キー・ファイル
－システム属性キーで暗号化
817

【図３６】


ソース・コンピュータ
1651
キー・ファイル
－製品キー
－顧客キー
－クリア計算機ＩＤ
－試用期間データ
－エクスポート・カウンタ
1653
キー
1659
暗号解読操作
1657
エクスポート・カウンタを修正
1661
キー
1662
計算機ＩＤファイル
－計算機ＩＤ
－試用期間データ
1665
暗号解読操作
1663
転送キー
1665
暗号化操作
1668
転送キー
1671
暗号化操作
1675
メモリ媒体にコピー
1679
メモリ媒体にコピー
1681
メモリ媒体
1677
メモリ媒体
1677

【図３７】



フロントページの続き

(72)発明者　ハドソン・ダブリュー・フィリップス
アメリカ合衆国80301　コロラド州ボウルダー　ジェームストン・ストリート　4725

(72)発明者　ロバート・エフ・プライアー
アメリカ合衆国80503　コロラド州ロングモント　マウント・ミーカー・ロード　7380